

作 者 简 介

张贤科,清华大学教授,博士导师。1944年2月29日生于安徽灵璧,祖籍河南开封。中国科学技术大学数学系毕业(1969北京),后取得硕士和博士学位并长期任教于该校。1993年任清华大学国际理论物理中心研究员(UNESCO,意大利)。多次较长时期赴美、欧作研究工作。任美国数学会会员,美国、德国《数学评论》长期评论员。曾获"中国科学院科技进步奖"(1988)、"国家自然科学奖"(1990),及"做出突出贡献的中国博士学位获得者"称号(1991)。长期从事代数数论等研究和教学,在《中国科学》,《美国数学会刊》,美国《数论杂志》等学术刊物上发表学术论文50多篇。在多类代数数域和函数域的分类、类群、类数、密度、相对扩张、种域理论等多方面取得许多远远超过国外的成果,被引用很多。

引　言

本书是在“1996 年全国数学研究生暑期学校”(在北京大学)讲义的基础上,结合在中国科学技术大学与清华大学的研究生课讲稿编写而成.目的是尽快引导读者到达代数数论这一极重要的现代数学领域.力求清晰简洁地从现代数学的角度阐释代数数论的基础,并且进入更深层主要理论.写作中融进了长期教学和研究中的感悟和想法,参阅了国际近期主要著作.

代数数论可以说就是古典数论的现代化,是现代数学最重要的分支之一,处于当代最活跃的数学前沿.已有多项历史性成果连续获得 Fields、Wolf 等大奖,Fermat 大定理的证明更是震动了整个世界.信息和计算机时代的到来更突出了它的实际应用意义.另一方面,这一领域的入门尚不是太难,研究对象在开始还是比较具体的,有路可循.历史上,数论中的概念和发现常常是推动数学发展的强大原动力.例如现在数学家们广泛使用的域、环、理想等概念,就是上世纪末代数数论中产生的.数论被称为“数学的皇后”.这也许就是原因之一.数论研究对象之基本,方法之优美,问题之神奇,意境之深远,也应是原因.当然,数论也广泛吸收其它领域的新概念方法而不断发展自身.例如,代数和拓扑方法的巨大影响,导致了 20 世纪数学的“现代化”,这一“现代化”对数论也有重大影响.现在在代数数论中,

代数、分析、几何(拓扑)这数学的三要素几乎有同样的重要性.

自然数,整数,到有理数,在很长的历史时期是数学的主要研究对象.整数全体 $\mathbf{Z}$ 是环,有理数全体 $\mathbf{Q}$ 是域.但后来人类终于陆续发现了 $\sqrt{2}$,$\sqrt{2+\sqrt{3}}$ 这样的无理数,还发现了 $i=\sqrt{-1}$ 这样的虚数.这些都是代数数.代数数(Algebraic Number)就是满足代数方程(即 $\mathbf{Q}$ 上的多项式方程)的复数(不一定能用根式写出来).在本来的意义上,代数数论就是关于代数数(或代数数域)的理论.它以理想的理论和方法为基本特征,是古典数论(即 $\mathbf{Z}$ 和 $\mathbf{Q}$ 的理论)到近代的自然发展.代数数论的研究领域和理论已经极大的拓展,现已包括各种局部域、代数函数域,算术代数几何(特别是椭圆曲线等曲线的算术理论),各种 Zeta-函数,L-函数,模形式理论,一些表示理论等等.

一般认为代数数论起始于高斯(C. F. Gauss 1777～1855),他研究了 $ax^2+bxy+cy^2$ 这样的二次型(相当于二次域)和分圆域.他 22 岁时的天才著作《Disquisitiones Arithmeticae》一书开辟了自Euclid和 Diophantus 以来数论的新历史阶段.他引入了同余概念,给出二次互反律许多证明.

代数数论的系统理论创始于德国数学家库默尔(E. E. Kummer 1810～1893).它从诞生之日起至今,始终与费尔马大定理结下不解之缘.现简述这段渊源,也就是代数数论的传奇历史.

费尔马(Pierre de Fermat 1601～1665)是法国业余数论学家.约于 1637 年在古希腊数学家丢番图(Diophantus)所著《算术》一书的页边上,费尔马写下了著名猜想:"分一个立方为两个立方之和,或分一个四次方为两个四次方之和,或一般地分任一高于二次的幂为两个同次幂之和,均是不可能的.对此我已发

现了真正奇妙的证明．但此页边太窄容不下”．这一猜想后来被称为费尔马大定理．即 $n \geqslant 3$ 时(费尔马)方程

$$a^n + b^n = c^n$$

无非零整数解 a,b,c. 对 $n=4$ 情形由费尔马证明(1640 左右). 1753 年 $n=3$ 的情形由欧拉(Euler)基本证明. 1825 年 $n=5$ 情形由 S. Germain(对 $abc \not\equiv 0 \pmod n$)，Dirichlet 和 Legendre 证明. 1839 年 $n=7$ 情形由 G. Lame 证明．200 年间基本只证明了这四种情形. 值得注意的是，在 $n=4$ 情形被证明之后，费尔马大定理归结为只要对奇素数 $n=p$ 证明即可．

1847 年 3 月 1 日(星期一)巴黎科学院会议上，拉梅(G. Lame)宣布他证明了费尔马大定理，方法是用复数分解

$$c^p = a^p + b^p = (a+b)(a+\zeta b)(a+\zeta^2 b)\cdots(a+\zeta^{p-1}b),$$

其中 ζ 是 p 次本原单位根(例如 $\zeta = \exp(2\pi i/p)$). Lame 想用复数因子分解的唯一性，右边各因子是互素的，积为 p 次幂，推出各因子均为 p 次幂，再导出矛盾完成证明．Lame 的报告引起了激烈的争论．Liouville 立即起来反对，说唯一分解律对复数不一定成立. Cauchy 等支持 Lame，他们在后来的数周内给出许多“证明”，还向科学院存入“秘密案袋”以备将来查优先权．激烈混乱的争论直到 5 月 24 日，Liouville 宣读了 Kummer 来信．信中说，复数的唯一分解律是不成立的，随信附上三年前发表的证明；不过这可以通过引入“理想数”来挽救，“理想数”满足唯一分解律；由此可以对许多情形证明费尔马大定理．Kummer 由此很容易对 100 以内的 n(除 37,59,67 外)证明了费尔马大定理．Kummer 对分圆域 $\boldsymbol{Q}(\zeta)$ 进行了深入的研究．后由德国 J. W. R. Dedekind(1831～1916)发展到一般数域，奠定了代数数论系统的理论基础. Dedekind 的理论作为德国 Dirichlet (1805～1859)所著《Vorlesungen uber Zahlentheorie》一书的附

录发表(1894),这本书基于 Euler 等式开创了数论的解析方法,后来发展出各种 Zeta-函数和 L-函数理论.

对于费尔马大定理,后来的深入研究得到了许多结果.下述每一个都是定理成立的充分条件:

(1) $h(p)\not\equiv 0(\mathrm{mod}\ p)$,其中 $h(p)$ 为 $Q(\zeta)$ 的类数;

(2) Bernoulli 数 $B_2,\cdots,B_{p-3}$ 均非 p 的倍数;

(3) $B_{2p},\cdots,B_{(p-3)p}$ 均非 p^3 的倍数,且 p 次分圆域最大实子域的类数也非 p 的倍数.借助于计算机,到 1993 年已对 4 000 000 以内的素数 p 验证了费尔马大定理.1983 年德国 Gerd Faltings 证明了 Mordell 猜想(即亏格大于一(约相当于次数大于 4)的曲线只有有限个有理点),从而证明了费尔马方程最多只有有限个非零整数解.这被认为是算术代数几何的巅峰.1993 年 6 月 23 日,普林斯顿大学来自英国的怀尔斯(Andrew J. Wiles 1953.4.11～)在英国剑桥牛顿数学科学研究所举行的研讨班上,宣布证明了费尔马大定理.引起了整个世界的震动.但不久此证明被发现有漏洞.怀尔斯最终在 1994 年 9 月 19 日的思维闪电中找到了迷失的钥匙,完成了这一有重大历史意义的证明.他是证明了 Taniyama 猜想(即椭圆曲线均为模曲线),再由 Ribet 的结果得到费尔马大定理.本书在第七章和第九章最后对费尔马大定理的证明有所介绍.

上世纪末,德国希尔伯特(David Hilbert 1862～1943)在编写数论报告《Zahlbericht》后,洞察到数域的类群与其 Abel 扩张间的关系,猜想到著名的"类域论"(1898).这是二次和高次互反律的自然推广.希尔伯特在第二次国际数学家大会(巴黎,1900)上,提出了新世纪面临的著名的 23 个问题,其中问题 9 至 12 来自代数数论.问题 9 和 12 是关于类域论的.Furtwangler、高木贞治(Takagi,1920)、E. Artin(1927)完成了类域论的理论

(1940 由 Chevalley 算术化). 类域论被称为数学各种理论中体系最完美的一种. 但类域的构作问题还有很长的路.

Hensel 在 1902 年建立了 p-adic 数理论,开创了局部域的方法和数论. 由此发展出关于局部和整体关系的 Hasse 原则(1923). 继而 Chevalley1936 年引入伊代尔(Idele)改写类域论. Weil 稍后引入阿代尔(Adele)证明 Riemann-Roch 定理. 此外,有限域上的代数函数域理论与代数数域理论有平行和互相推动的发展,前者与代数几何有很深关系,其上的 Riemann 猜想和 A. Weil 猜想已由 Weil(1948)和 P. Deligne(1973)解决.

近期以来,代数数论正经历着历史性惊人的发展. 正象从怀尔斯对费尔马大定理的证明可以看到的;已经取得伟大的成就,但还有更广袤的领域待征服. 有古老的猜想(像 Gauss 猜想,虚部分的解决已数次震动数学界,实部分远未突破);也有新问题,新天地.

本书试图引导读者进入这片美好的天地. 前三章以理想论阐述代数数域的基本性质,论述整数环和整性,诺特环和戴德金环,用局部化方法阐述素理想在扩域中的分解,分析了分解群,惯性群等. 以理想论作开始,是为了便于掌握,也与历史发展一致. 第四,五两章在前述基础上发展了赋值论,完备化,和局部域的扩张等进一步的理论,并以此讨论了差分和判别式. 这些已成为现代数论的基本方法和语言. 第六章简洁地证明了类数有限性定理和单位定理. 第七章讨论了二次域的单位群,欧几里得域问题和类数;讨论了分圆域的基本数论. 第八章给出域的特征群与域的结构关系,Zeta-函数,L-函数,类数公式. 这些是解析方法的基础. 第九章阐述了伊代尔群,射线(广义)理想类群,整体和局部类域论,Hilbert 类域等较深的内容. 书中有不少注记,举例和练习题. 总起来看,切实掌握本书的内容后,

可使读者进入研究工作和进一步学习的新层次．本书可作为数学研究生或高年级本科生等的教材或参考．预备知识为初等数论和抽象代数的基本知识，包括简单的伽罗华理论．

全国数学研究生暑期学校的组织者，国家自然科学基金委数理学部负责同志，以及湖南教育出版社，分别对暑期讲学和本书出版给予极大支持，作者深表感谢．作者也借此机会对在代数和数论研究中曾热情支持帮助过我的中国科技大学的曾肯成教授、冯克勤教授和陆洪文教授深表感谢．

由于水平有限，时间紧迫，定有许多不当之处．诚恳欢迎批评指正．

张贤科

1997 年 10 月于清华园

目　录

预备知识概述

集合、群、环、域、模等

集合与映射的知识假定读者已熟悉．以 $A-B$ 表示 B 在 A 中的补集．集合 A 的元素个数或基数记为 $|A|$ 或 $\# A$. A 与 B 的笛卡尔积即为集合 $A\times B=\{(a,b)|a\in A,b\in B\}$. 映射 $f: A\to B$ 称为**单射**(injective)是指 $f(a)=f(b)$ 蕴含着 $a=b$. f 称为**满射**(surjective)是指对任意 $b\in B$ 总有 $a\in A$ 使 $f(a)=b$. 若 f 既是单射又是满射，则称 f 为**双射**或 1：1 对应．映射 $f: A\to B$ 和 $g: B\to C$ 的复合（或称乘积）记为 $g\circ f$ 或 gf，它映 a 为 $g(f(a))$. 设 S 是 A 的子集，则映射 $f: A\to B$ 决定了一个映射 $g: S\to B$，由 $g(s)=f(s)$ 定义. 映射 g 称为 f（到 S 上）的限制，f 称为 g（到 A 上）的延拓.

群、环、域假定读者已知．简单地说．**群**(Group)就是一个集合 G，在其中可进行一种运算及其逆运算．确切言之，群 G 就是一个集合 G，定义有某二元运算 $*$（可能是乘法 $\times$，或加法 $+$ 等）满足如下 4 条：(1)封闭性，即对任意 $a,b\in G$ 总有 $a*b\in G$；(2)结合律，即 $a*(b*c)=(a*b)*c$；(3)存在单位元 e，即有 $e\in G$ 使 $a*e=e*a=a$；(4)存在逆元，即对任意 $a\in G$ 总存在 $b\in G$（称为 a 的逆元）使 $a*b=b*a=e$（对任意 $a,b,c\in G$）. 若运算 $*$ 是乘法，常称 G 为乘法群，记单位元 e 为 1，记 a 的逆

元为a^{-1}. 若运算$*$还满足交换律,即$a*b=b*a$对任意$a,b\in G$成立,则称G为阿贝尔(Abel)群或交换群. Abel群的运算$*$常常记为加法(+),称为加法群,单位元e记为0(称为零元),a的逆元记为$-a$(称为负元). 若H为群G的子群(即为G的子集且对G的运算为群),则H的指数为$(G:H)=|G|/|H|$. 若A,B为两个加法群则记其和为$A+B=\{a+b|a\in A,b\in B\}$.

环(Ring)就是一个内有加、减、乘法的集合. 确切言之,环A就是定义有加法和乘法两个运算的集合, 对加法为Abel群, 对乘法为半群(即只满足封闭性和结合律)且乘法对加法有分配律. 若对乘法有单位元,则称为含幺环. 若环的乘法满足交换律,则称之为交换环. 本书中的环均指含幺交换环. 如果环A中任两个非零元素之积均非零,则称A为无零因子环(或有消去律环),也称为整环或整区(domain). 环A中的乘法可逆元称为环的单位,全体单位记为A^*,是乘法群,称为单位群. 对于环A,以$A[X]$记A上不定元X的多项式集,是一个环. 以$A[X_1,\cdots,X_n]$记n元多项式环. 以$A[[X]]$记形式幂级数环. 设环$A\subset B$而$x\in B$,则以$A[x]$记A和x生成的B的子环,即以A中元素为系数的x的多项式全体. 同样以$A[x_1,\cdots,x_n]$记A和$x_1,\cdots,x_n\in B$生成的子环.

域(Field)就是一个内有加、减、乘、除法的集合. 确切言之,域F就是一个环且其非零元集是乘法Abel群. 若K为域F的子域(即子集且对F的运算为域),则称F为K的扩域或扩张(extension). 此时F自然是K上的线性空间,其维数称为**扩张次数**,记为$[F:K]$; F作为K上线性空间的基称为它的K-**基**. 次数有限的扩张称为有限扩张. 特征为0的域(可认为)即是有理数域$\boldsymbol{Q}$的扩域,特征为p(素数)的域即是$\boldsymbol{F}_p=\boldsymbol{Z}/p\boldsymbol{Z}$的扩域. 有限域$F$必是特征为(某素数)$p$的域,其元素个数为$p$

的幂 $q=p^n$，记 $F=\mathbf{F}_q$. $\mathbf{F}_q$ 的非零元全体是 q-1 阶乘法循环群．域 F 上多项式形式环记为$F[X]$，其分式域(商域)$F(X)$称为有理式(形式)域，或有理函数域．

模(Module)是加法群或线性空间的自然推广．线性空间的基域如果改而为环，就是模．确切言之，设 A 为环，M 为一加法(Abel)群，若 A 与 M 的元素有运算(即有映射 $A\times M\to M$，$(a,x)\longmapsto ax$)且满足

$$a(x+y)=ax+ay, \qquad (a+b)x=ax+bx$$
$$(ab)x=a(bx), \qquad 1x=x$$

(对任意 $a,b\in A, x,y\in M$)，则称 M 是 A-模或 A 上的模．例如，加法群均为 $\mathbf{Z}$-模，域 F 上线性空间均为 F-模．对模 M 的任意子集 $S=\{x_i\}$，形如 $\sum\limits_i a_ix_i(a_i\in A)$ 的有限和(A-线性组合)全体 N 是一个 A-模，称为 S 生成的子模，记为 $N=AS$，它恰为含$\{x_i\}$的最小子模，$\{x_i\}$ 称为它的**生成元系(集)**．由一个元素 x 生成的子模记为 Ax. 如果 M 有一个有限生成元系，则 M 称为**有限生成的**．设 M 有一个有限生成元系 $\alpha_1,\cdots,\alpha_n$，且 M 中任一元可唯一地表示为 $a_1\alpha_1+\cdots+a_n\alpha_n(a_1,\cdots,a_n\in A)$，则称 M 为**自由 A-模**，**秩**为 n；此时记 $M=A\alpha_1\oplus\cdots\oplus A\alpha_n$，且称$\{\alpha_1,\cdots,\alpha_n\}$为 M 的 A-**基**．例如域 F 上向量空间均是自由 F-模．$\mathbf{Z}$ 是自由 $\mathbf{Z}$-模．$\mathbf{Z}/m\mathbf{Z}$ 不是自由 $\mathbf{Z}$-模. 如果一个 Abel 群 G 作为 $\mathbf{Z}$-模是有限生成的，则称此群是有限生成的．

现设 A 为主理想环，M 是秩为 n 的自由 A-模，N 是 M 的子模，则 N 也是自由 A-模，其秩 $q\leqslant n$. 而且存在着 M 的 A-基$\{\alpha_1,\cdots,\alpha_n\}$使得$\{a_1\alpha_1,\cdots,a_q\alpha_q\}$为 N 的 A-基，其中 a_i 整除 a_{i+1}均为 A 中元．由此可知，任一有限生成的 A-模 E 必同构于 $A/(a_1)\oplus\cdots\oplus A(a_q)\oplus A^r$，其中$(a_1)\supset\cdots\supset(a_q)$为 A 的主理想，A^r

$=A\oplus\cdots\oplus A$ 称为其自由部分，$A/(a_1)\oplus\cdots\oplus A/(a_q)$称为其挠（或扭，torsion）部分. 特别地，无挠有限生成 A-模必是自由模.

如果 B 为环，又为 A-模；且 $a(xy)=(ax)y=x(ay)$（对任意 $a\in A,x,y\in B$），则称 B 为 A-**代数**或 A 上的代数. 例如 $\mathbf{Z}[X]$ 是$\mathbf{Z}$-代数. 两个环 A,B 间的映射 $f:A\to B$ 称为同态，如果它满足 $f(a+b)=f(a)+f(b),f(ab)=f(a)f(b),f(1)=1$（对任意 $a,b\in A$）. 此时也称 B 为 A-代数，事实上定义运算 $ax=f(a)x$，即得上述意义下的代数. 环的双射同态称为同构.

环 A 的一个**理想**（Ideal）I 就是 A 的一个加法子群，且还满足吸收律：对任意 $a\in A$ 和 $b\in I$ 有 $ab\in I$. 注意理想 I 是 A-模. A 和 $\{0\}$ 均为理想，称为平凡理想. 域只有平凡理想. 对环 A 的任意子集 $\{b_i\}$，形如 $\sum_i a_ib_i$ 的有限和全体（$a_i\in A$）是一个理想，称为 $\{b_i\}$ 生成的理想. 由一个元素 b 生成的理想称为主理想，记为 Ab 或 (b). 显然 $(1)=A$. **主理想（整）环（PID）**就是所有理想均为主理想的整环. 例如 $Z,F[X]$（域上多项式环）均是. 注意在 Z 中有 $(3)\supset(6)$. 因此在一般的环中，若理想 $I\supset J$，则记为 $I|J$.

商环、商模等概念是基于**商群**的. 设加法群 G 有子群 H，可以按 H 对 G 的元素分类（称为模 H 的同余类）：a,b 属于同一类当且仅当 $a-b\in \mathrm{H}$，记为 $a\equiv b(\mathrm{mod}\ H)$. a 所在的同余类（称为 a 所代表的类）即为 $\bar{a}=a+H=\{a+h|h\in H\}$. 同余类全体记为$G/H$，这是一个加法群（称为 G 对模 H 的商群，或同余类群），运算定义为 $\bar{a}+\bar{b}=\overline{a+b}$或$(a+H)+(b+H)=(a+b+H)$. 对于（非Abel）乘法群 G 及其子群 H，也可类似地构作商群，但要求 H 为**正规子群**（即 $aH=Ha$ 对任意 $a\in \mathrm{G}$）才可使同余类的运算定义有意义，即定义 $a\equiv b(\mathrm{mod}\ H)$为 $ab^{-1}\in H$，$\bar{a}=$

aH，$\bar{a}\bar{b}=\overline{ab}$. 设 $f: G\to G'$ 为加法群间的映射，若 f"保持加法"，即 $f(a+b)=f(a)+f(b)$（对任意 $a,b\in A$），则称 f 为同态映射. 称 G' 中 0 的原象 $\mathrm{Ker}(f)=\{a\in A\mid f(a)=0\}$ 为 f 的核，核是子群. 总有群同构 $G/\mathrm{Ker}(f)\cong \mathrm{Im}(f)=\{f(a)\mid a\in A\}$. 对于乘法群，可类似定义同态 $f: G\to G'$ 为满足 $f(ab)=f(a)f(b)$ 的映射，核 $\mathrm{Ker}(f)=\{a\in A\mid f(a)=1\}$ 为正规子群，也总有同构 $G/\mathrm{Ker}(f)\cong \mathrm{Im}(f)$.

设 A 为环，I 为其一理想. 于是 A 为加法群，I 为其子群，故可如上构作（加法）商群 A/I. 再定义 t 同余类的乘法 $\bar{a}\bar{b}=\overline{ab}$，则 A/I 成为环，称为商环. 有自然同态满射 $f: A\to A/I, a\longmapsto \bar{a}$. 商环 A/I 的理想均形如 J/I，其中 J 为 A 中含 I 的理想. 当且仅当 I 为**极大理想**（即 I 与 A 之间无理想）时，A/I 为域. 当且仅当 I 为**素理想**（即 $xy\in I$ 蕴含 $x\in I$ 或 $y\in I$）时，A/I 为整环. 环的同态映射 $f: A\to B$ 的核 $\mathrm{Ker}(f)=\{a\in A\mid f(a)=0\}$ 为 A 的理想，总有环同构 $A/\mathrm{Ker}(f)\cong \mathrm{Im}(f)$.

设 M 是 A-模，N 是其子模（即 N 是其子集且对原有运算是 A-模）. 于是 M 为加法群，N 为其子群，故可如上构作（加法）商群 M/N. 再定义 A 的作用为 $a\bar{x}=\overline{ax}$，则 M/N 成为 A-模，称为**商模**. A 上模 M 和 M' 间的映射 $f: M\to M'$ 如果满足如下条件则称为（模的）同态或 A-线性映射：$f(x+y)=f(x)+f(y)$，$f(ax)=af(x)$（对任意 $a\in A, x,y\in M$）. 核 $\mathrm{Ker}(f)=\{x\in M\mid f(x)=0\}$ 为 M 的子模，总有模的同构（双射同态）：$M/\mathrm{Ker}(f)\cong \mathrm{Im}(f)$.

下面介绍**整除性**. 设 A 为整环，$K=\{a/b\mid a,b\in A, b\neq 0\}$ 为其分式域. 对于 $x,y\in K$，如果存在 $a\in A$ 使 $y=ax$，则称 x

整除 y，x 是 y 的因子，y 是 x 的倍(元)，记为 $x|y$. 我们称 x 的倍元全体 Ax 为 x 生成的(分式)理想. 显然 $x|y$ 相当于 $y\in Ax$ 或 $Ay\subset Ax$. 若 x 整除 y，且 y 整除 x，则称 x 与 y 互为**结合**元素，这也相当于 $Ay=Ax$，与 1 相结合的元素恰为 A 的单位(即 A 中可逆元). (非零的)两个相结合元素的商也为 A 的单位. 设 p 为 A 中非零元，若 p 无真因子(即 p 只有单位及与自身相结合的因子)，则称 p 为**不可约元**. 若 A 中非零元均可唯一表示为有限个不可约元之积(不计因子次序和单位因子)，则称 A 为**唯一析因(整)环**(UFD). 主理想(整)环均为唯一析因环.

符 号 表

$\boldsymbol{C}$	复数域	$\boldsymbol{F}_q$	q 元有限域
$F[X]$	F 上多项式环	$\boldsymbol{I}(\mathfrak{m})$	与 $\mathfrak{m}$ 互素的理想集
$\boldsymbol{J}(k)$	k 的 Idele 群	N	自然数集
O_K	数域 K 的整数环	$\boldsymbol{P}_{\mathfrak{m}}$	射线主理想群
Q	有理数域	R	实数域
Z	(有理)整数环	$(-,K/k)$	*Artin* 符号

第一章　数域与数环

§1.1　代数整数

有理数域$\boldsymbol{Q}$的有限扩域K称为**代数数域**,或**数域**. 这也就是说,K是复数域$\boldsymbol{C}$的一个子域,且K在$\boldsymbol{Q}$上的次数$[K:\boldsymbol{Q}]$(即K作为$\boldsymbol{Q}$上的线性空间的维数)是有限的.

例 1　(**二次域**)设$K=\boldsymbol{Q}(\sqrt{m})=\{a+b\sqrt{m}\mid a,b\in\boldsymbol{Q}\}$,其中$m$是一无平方因子整数. 则$K$是二次数域,$\{1,\sqrt{m}\}$是$K$的$\boldsymbol{Q}$-基. 反之,任意二次数域$K$必可表示为这种形式:任取$\alpha\in K-\boldsymbol{Q}$(即属于$K$而不属于$\boldsymbol{Q}$),则$1,\alpha$线性无关,而$1,\alpha,\alpha^2$线性相关(因维数为2),故有$a\alpha^2+b\alpha+c=0$, $a,b,c\in\boldsymbol{Z}$(整数环);从而$\alpha=(-b\pm\sqrt{b^2-4ac})/2a$,再取$m$为$b^2-4ac$无平方因子部分即可.

例 2　(**分圆域**)设$m>2$是一正整数. 记$\zeta=\zeta_m=\exp(2\pi i/m)$,则

$$K=\boldsymbol{Q}(\zeta_m)$$

称为(m级)分圆域. 注意$1,\zeta,\zeta^2,\cdots,\zeta^{m-1}$恰为$X^m-1$的$m$个

复根，称为 m 次单位根，它们构成一个乘法循环群．此群恰有 $\varphi(m)$ 个生成元(称为 m 次本原单位根)：ζ^k ($k<m$ 且与 m 互素)，这里 φ 是 Euler 函数．将证明 $\boldsymbol{Q}(\zeta_m)$ 的次数是 $\varphi(m)$，$\varphi(m)$ 个本原单位根恰好是 $\boldsymbol{Q}$ 上一个 $\varphi(m)$ 次不可约多项式 $\Phi_m(X)$ (称为分圆多项式)的复根．

若复数 α 是一有理系数多项式 $f(X)\in\boldsymbol{Q}[X]$ 的根，即 $f(\alpha)=0$，则称 α 为**代数数**(algebraic number)．此时也可设 $f(X)\in\mathbf{Z}[X]$ 为整数系数多项式，即 α 满足(代数)方程

$$a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0=0 \quad (a_n,\cdots,a_0\in\mathbf{Z}). \quad (1)$$

如果复数 α 是首一(即最高次项系数是 1)的整数系数多项式的根(即(1)式中 $a_n=1$)，则称 α 为**代数整数**(algebraic integer)或**整数**．为了区别，$\boldsymbol{Q}$ 中的整数有时被称为有理整数．一般地，若某元素 α 是域 K 上多项式 $f(X)\in K[X]$ 的根，则称 α 为 K 上的**代数元素**；若 $f(X)$ 是不可约的，则称 $f(X)$ 为 α 在 K 上的的极小多项式．例如，例 1 中 α 的极小多项式为 aX^2-bX+c；例 2 中 ζ_m 的极小多项式为 $\Phi_m(X)$．

一个代数数域 K 中的元素 α 均是代数数，这是因为 K 的次数有限，故 $1,\alpha,\alpha^2,\alpha^3,\cdots$ 之中，必有有限个元素的有理系数线性组合为 0．有理整数，及 $\sqrt{2}$，$\sqrt[3]{5}$，ζ_m 均为代数整数．代数整数是有理整数的自然推广．可以证明，有许多代数数(和代数整数)不能"用根式表示出来"(Galois)．

对每一个代数数 α，都可乘以一个有理整数 a 使 $a\alpha$ 为代数整数．事实上，若 α 满足(1)式，则两边乘以 $a=a_n$ 的 $n-1$ 次方，即得

$$(a\alpha)^n+a_{n-1}(a\alpha)^{n-1}+\cdots+a_1a^{n-2}(a\alpha)+a_0a^{n-1}=0$$

从而知 $a\alpha$ 为整数．例如若 $5\alpha^3-2=0$，$\alpha=(2/5)^{1/3}$，则 $5\alpha=(2\times5^2)^{1/3}$ 为整数．

一个代数数域 K 中的代数整数全体记为 O_K. 它将是代数数论的主要研究对象，这正像 $\mathbf{Z}$ 是古典数论的主要研究对象一样. 首先我们要证明 O_K 是一个环. 为此只要证明它对加法和乘法封闭，即要证明：任两个代数整数的和与积均为代数整数. 例如对 $\alpha=\sqrt{2}+\sqrt{3}$，由 $\alpha^2=5+2\sqrt{6}$，及 $(\alpha^2-5)^2=24$，可知 α 为代数整数. 但对一般情形，很不易证明. 为此最好是用"线性化"方法，即把 O_K 看作"好像 $\mathbf{Z}$ 上的线性空间"(确切地说，O_K 是"$\mathbf{Z}$ 上的模"). 以下定理本质上就是线性代数中的一个定理：线性变换 T 的特征多项式 $f(X)$ 是 T 的零化多项式. 注意 $f(X)$ 是首一的.

定理 1 对复数 α，以下各命题等价：

(i) α 为(代数)整数.

(ii) 环 $\mathbf{Z}[\alpha]$ 的加法群是有限生成的.

(iii) 存在环 $B\subset \mathbf{C}$，其加法群是有限生成的，且含 α.

(iv) 存在非零加法群 $B\subset \mathbf{C}$，是有限生成的，且 $\alpha B\subset B$.

证明 (i)⇒(ii)：设 α 满足方程(1)而 $a_n=1$. 于是 $\alpha^n=-a_{n-1}\alpha^{n-1}-\cdots-a_1\alpha-a_0$ 是 $1,\alpha,\alpha^2\cdots,\alpha^{n-1}$ 的 $\mathbf{Z}$-线性组合. 故 α^{n+1}，α^{n+2} 等也是它们的 $\mathbf{Z}$-线性组合. 由此易知 $\mathbf{Z}[\alpha]$ 的加法群可由 1，$\alpha,\alpha^2\cdots,\alpha^{n-1}$ 生成.

(ii)⇒(iii)⇒(iv)：显然.

(iv)⇒(i)：设加法群 B 由 $\alpha_1,\cdots,\alpha_n$ 生成(这里的情形类似于 B 是"线性空间"，$\alpha_1,\cdots,\alpha_n$ 是"基". 而 $\alpha B\subset B$ 说明 α 是 B 的一个"线性变换"：$x\longmapsto \alpha x$. 于是其特征多项式 $f(X)\in \mathbf{Z}[X]$ 是首一的且 $f(\alpha)=0$). 那么由 $\alpha B\subset B$ 知道 $\alpha\alpha_i\in B$，从而是 $\alpha_1,\cdots,\alpha_n$ 的 $\mathbf{Z}$-线性组合($1\leq i\leq n$)：

$$\alpha\alpha_1=a_{11}\alpha_1+\cdots+a_{1n}\alpha_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\alpha\alpha_n=a_{n1}\alpha_1+\cdots+a_{nn}\alpha_n$$

(a_{ij}均属于 $\mathbf{Z}$). 记方阵 $M=(a_{ij})$, I 为 n 阶单位方阵,则上式可写为

$$(\alpha I)\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=\begin{pmatrix}\alpha\alpha_1\\ \vdots\\ \alpha\alpha_n\end{pmatrix}=M\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix},$$

$$(\alpha I-M)\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=0\ .$$

在上式左边乘以(αI-M)的伴随方阵(一个方阵 $T=(t_{ij})$ 的伴随方阵定义为 $T^*=(s_{ij})$,其中 s_{ij}为 t_{ji}的代数余子式,有性质 $TT^*=T^*T=\det(T)$为 T 的行列式),记

$$f(\alpha)=(\alpha I-M)^*(\alpha I-M)=\det(\alpha I-M)$$
$$=\alpha^n+\cdots+a_1\alpha+a_0$$

(a_i 均属于 $\mathbf{Z}$),则

$$f(\alpha)\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=\begin{pmatrix}f(\alpha)\alpha\\ \vdots\\ f(\alpha)\alpha_n\end{pmatrix}=0.$$

即 $f(\alpha)\alpha_i=0(1\leq i\leq n)$,因 $\alpha_1,\cdots,\alpha_n$ 不全为零,故 $f(\alpha)=0$,从而知 α 是代数整数. □

系 1 任两个代数整数的和与积均为代数整数. 特别知,代数整数全体是一个整环;每个数域 K 中代数整数全体 O_K 是一个整环(称为 K 的整数环).

证明 若α，β为代数整数，由定理1知环$\mathbf{Z}[\alpha]$，$\mathbf{Z}[\beta]$的加法群均是有限生成的，于是环$\mathbf{Z}[\alpha,\beta]$也是有限生成的(若$\{\alpha_i\}$，$\{\beta_j\}$是前两加法群的生成元系，则$\{\alpha_i\beta_j\}$显然是$\mathbf{Z}[\alpha,\beta]$的生成元系). 因为$\mathbf{Z}[\alpha,\beta]$含$\alpha+\beta$，$\alpha\beta$，从而由定理1知这二个元素为代数整数. □

整数环O_K是一个加法群，从而是一个$\mathbf{Z}$-模. 将证明它是秩为n的自由$\mathbf{Z}$-模

二次域中的整数

二次(数)域即有理数域$\boldsymbol{Q}$的二次扩张，总可表为

$$K=\boldsymbol{Q}(\sqrt{m})=\{a+b\sqrt{m}\mid a,b\in\boldsymbol{Q}\},$$

其中m是一无平方因子整数. 我们来求K的整数环O_K. 设$\alpha=a+b\sqrt{m}$为整数($a,b\in\boldsymbol{Q}$)，显然α满足方程

$$X^2-2aX+(a^2-mb^2)=0.$$

注意$\bar{\alpha}=a-b\sqrt{m}$也满足此方程，故$\bar{\alpha}$也是整数. 于是$\alpha+\bar{\alpha}$和$\alpha\bar{\alpha}$，即$2a$和a^2-mb^2，均整数，又是有理数，故

$$2a\in\mathbf{Z},\quad a^2-mb^2\in\mathbf{Z}$$

于是$(2a)^2-m(2b)^2=4(a^2-mb^2)\in\mathbf{Z}.$，故$m(2b)^2\in\mathbf{Z}$. 我们断言$2b\in\mathbf{Z}$；否则$(2b)^2$的分母含平方因子，而$m$无平方因子，与$m(2b)^2\in\mathbf{Z}$矛盾. 于是可设$a=u/2$，$b=v/2$，$u,v\in\mathbf{Z}$. 则上式化为

$$u^2-mv^2\in 4\mathbf{Z}.$$

因此，若v为偶数，则u亦偶数，a,b均整数. 若v为奇数，则$v^2\equiv1\pmod{4}$；由上式知u为奇数而$m\equiv1\pmod{4}$. 这也就是说，在$m\equiv2$或$3\pmod{4}$时，$\alpha=a-b\sqrt{m}$为整数当且仅当a,b均有理整数. 而在$m\equiv1\pmod{4}$时，$\alpha=a+b\sqrt{m}=(u+v\sqrt{m})/2$

为整数当且仅当 u,v 同为偶数或同为奇数. 故有

定理 2 设二次域 $K=\boldsymbol{Q}(\sqrt{m})$，其中 m 为无平方因子整数. 则 K 的整数环 O_K 如下：

(i) 当 $m\equiv 2$ 或 $3(\mathrm{mod} 4)$时，

$$O_K=\{a+b\sqrt{m}\mid a,b\in \mathrm{Z}\};$$

(ii) 当 $m\equiv 1(\mathrm{mod} 4)$时，

$$\begin{aligned} O_K &= \{\frac{u+v\sqrt{m}}{2}\mid u\equiv v(\mathrm{mod} 2),u,v\in \mathrm{Z}\} \\ &= \{a+b(\frac{1+\sqrt{m}}{2})\mid a,b\in \mathrm{Z}\}. \end{aligned}$$

定理 2 也可叙述为：O_K 的 **Z**-基(即作为 **Z**-模的基)在上述两种情形下分别为(i)$1,\sqrt{m}$；(ii)$1,(1+\sqrt{m})/2$.

将在第 7 章中证明，分圆域 $L=\boldsymbol{Q}(\zeta_m)$中的整数恰为 $a_0+a_1\zeta_m^1+\cdots+a_s\zeta_m^s$，$s=\varphi(m)-1,a_i\in\mathbf{Z}$. 也就是说，$\{1,\zeta_m,\cdots,\zeta_m^s\}$是 O_L 的 **Z**-基.

§1.2 整元素

整数的概念极易推广为“整元素”的概念.

定义 1 设 A 为含幺交换环，含于交换环 C 中，$\alpha\in C$. 若 α 满足 A 上某首一多项式 $f(X)\in A[X]$(或者说 α 是 $f(X)$的根)，则称 α 为 A 上的**整元素**(integral element)，或称 α 在 A 上**是整的，称 $f(x)=0$ 为 α 的整性方程**. 若环 B 中的所有元素在 A 上均是整的，则称环 B 在 A 上是整的. C 中在 A 上整的元素

全体称为 A 在 C 中的**整闭包**. 若此整闭包等于 A,则称 A 在 C 中是整闭的. 若 A 在其分式域中是整闭的,则称 A 是**整闭的**.

因此代数整数就是 $A=\mathbf{Z}$ 上的整元素. 和上节一样知:若 A 有分式域(也称商域)K,则对 K 上任意代数元 α,均存在某 $a\in A$ 使 $a\alpha$ 为 A 上整元素. 以下结果和证明与上节几乎完全相同,仅需注意上节说到加法群(即 $\mathbf{Z}$-模)处,现在换为 A-模.

定理 1 设 $A\subset C$ 均为含幺交换环,则对 $\alpha\in C$,以下各命题等价:

(i) α 为 A 上的整元素.

(ii) 环 $A[\alpha]$是有限生成的 A-模.

(iii) 存在环 $B\subset C$,使 B 是有限生成的 A-模且含 α.

(iv) 存在非零 A-模 $B\subset C$,使 B 是有限生成的 A-模,且 $\alpha B\subset B$.

系 1 设 $A\subset C$ 为交换环, 若 α, $\beta\in C$ 是 A 上整元素, 则 $\alpha\pm\beta$, $\alpha\beta$ 均为 A 上整元素. 特别知 C 中在 A 上整的元素全体为一个环.

系 2 (i)设 $A\subset C$ 为交换环,$\alpha,\beta\in C$. 若 α 在 A 上是整的,β 在 $A[\alpha]$上是整的,则 $A[\alpha,\beta]$是有限生成 A-模.

(ii)(整性的传递性)设 $A\subset B\subset C$ 为交换环. 若 B 在 A 上是整的,C 在 B 上是整的,则 C 在 A 上是整的.

证明 (i) 由定理 1 知 $A[\alpha]$ 是有限生成的 A- 模,设 $\alpha_1,\cdots,\alpha_n$ 是其生成元,即 $A[\alpha]=\sum_i A\alpha_i$. 又由定理 1 知 $A[\alpha,\beta]$ 是有限

生成的 $A[\alpha]$- 模，设其生成元为 $\beta_1,\cdots,\beta_m$，即 $A[\alpha,\beta]=\sum_j A[\alpha]\beta_j$. 于是 $A[\alpha,\beta]$ 作为 A- 模以 $\{\alpha_i\beta_j\}(1\leq i\leq n,1\leq j\leq m)$ 为生成元. 这由下式易知：

$$A[\alpha,\beta]=\sum_j A[\alpha]\beta_j=\sum_j(\sum_i A\alpha_i)\beta_j=\sum_{i,j}A(\alpha_i\beta_j).$$

(ii) 任取 $\alpha\in C$，则 α 在 B 上是整的，故有多项式

$$f(X)=X^n+b_{n-1}X^{n-1}+\cdots+b_0\quad(b_j\in B,1\leq i\leq n)$$

使 $f(\alpha)=0$. 令 $B'=A[b_0,\cdots,b_{n-1}]$，则有 $A\subset B'\subset B\subset C$. 上式说明 α 在 B' 上是整的. 又因 $b_i\in B$ 在 A 上均是整的，连续运用上述(1)知 $B'[\alpha]=A[b_0,\cdots,b_{n-1},\alpha]$是有限生成 A-模. 故 α 在 A 上是整的(定理 1). 即知 C 在 A 上是整的. □

命题 1 唯一析因整环是整闭的.

证明 设 A 为唯一析因整环，K 为其分式域，$\alpha\in K$ 在 A 上整，于是满足 A 上首一多项式：

$$\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0\qquad(a_i\in A).$$

设 $\alpha=a/b$，a，$b\in A$ 且互素，代入上式去分母得

$$a^n+a_{n-1}ba^{n-1}+a_1b^{n-1}a+a_0b^n=0,$$

故 $b|a^n$，从而 b 为单位(因 a 和 b 互素)，即 $\alpha=a/b\in A$. □

将上述整性运用到代数整数环 O_K 上，则易知有：

系 3 (i) $\boldsymbol{Q}$ 中的代数整数环即为 $\boldsymbol{Z}$.

(ii) 设 $K\subset L$ 为二数域. 则 O_L 恰为在 O_K 上整的 L 中元素全体. 即 O_L 是 O_K 在 L 中的整闭包.

(iii) O_K 在 K 中整闭(即在 O_K 上整的 K 中元素集恰为 O_K).

(iv) K 是 O_K 的分式域.

证明 (i) 由命题1即知. (ii) O_L 中元素均在 $\mathbf{Z}$ 上整,故在 O_K 上整. 反之若 $\alpha\in L$ 在 O_K 上整,则由系 2(2)知 α 在 $\mathbf{Z}$ 上整,即 $\alpha\in O_L$. (iii)设 $\alpha\in K$ 在 O_K 上整,则在 $\mathbf{Z}$ 上整,即 $\alpha\in O_K$. (iv) 设 $\alpha\in K$ 则存在 $a\in\mathbf{Z}$ 使 $a\alpha\in O_K$,故 α 属于 O_K 的分式域. □

现将上述整性运用到域 K 上,则易知有:

系 4 (i) 设 $A\subset B$ 为二整环,B 在 A 上是整的. 则 A 与 B 或同为域,或同非域.

(ii)α 是域 K 上整元素$\Leftrightarrow\alpha$ 是域 K 上代数元素. 这也相当于 $K[\alpha]=K(\alpha)$是 K 上有限维线性空间.

(iii) 设 α 是域 K 上代数元,β 是域 $K(\alpha)$上代数元,则 $A[\alpha,\beta]$是 K 的代数扩张.

(iv)设 $K\subset L\subset M$ 为三个域,且 L 是 K 的代数扩张,M 是 L 的代数扩张,则 M 是 K 的代数扩张且

$$[M:K]=[M:L][L:K].$$

证明 (i)设 A 为域. 任取 $0\neq\beta\in B$,则由定理1知 $A[\beta]$是有限维线性空间(即有限生成 A-模). β 定义了它的一个线性变换 $x\longmapsto\beta x$,是单射(因 B 是整环),故也是满射,从而存在 $\beta'\in A[\beta]$使 $\beta\beta'=1$. 即 β 可逆. 故 B 为域. 反之,设 B 是域. 任取 $0\neq\alpha\in A$,则 α 有逆元 $\alpha^{-1}\in B$,满足 A 上首一多项式

$$\alpha^{-n}+a_{n-1}\alpha^{-(n-1)}+\cdots+a_1\alpha^{-1}+a_0=0\quad(a_i\in A).$$

两边同乘以 α^{n-1}即得 $\alpha^{-1}\in A$,故 A 是域. (ii)—(iv)显然.

习　题

1. 设 A 为整环，K 为其分式域，L/K 为任一扩张，B 为 A 在 L 中的整闭包.

(1) 设 $\alpha \in K \cap B$，则存在 $c \neq 0 \in A$ 使 $c\alpha^n \in A(n=1,2,3,\cdots)$.

(2) 若 A 是整闭的，则 $K \cap B = A$.

(3) 若 A 是整闭的，$\alpha \in B$，则 α 在 K 上的首一极小多项式系数属于 A.

(4) 若 A 是整闭的，$f(X) \in A[X]$为首一多项式. 则 $f(X)$ 在 A 上不可约当且仅当在 K 上不可约.

(5) 若 L/K 是代数扩张，则 L 是 B 的分式域. 且 $\alpha \in L$ 均可表为 β/c，$\beta \in B$，$c \in A$.

§1.3　共轭与嵌入，迹与范

设 K 为域，L 和 L' 是 K 的两个扩张，φ: $L \to L'$ 为域的同构映射. 若 φ 限制到 K 上为恒等映射，则称 φ 为 K-同构(映射)，称 L 与 L' 为 K-同构或 **K-共轭**，也分别称为 K 上同构和共轭(conjugate over K). 对 $\alpha \in L$，称 $\varphi(\alpha)$ 为 α 的共轭元. 若 σ: $L \to C$ 为域的**嵌入**(即环的单同态，这里设 C 是 K 的一个扩张)且限制到 K 上为恒等映射，则称 σ 为 **K-嵌入**(K-Embedding)，此时 L 与 $\sigma(L)$是 K-同构(K-共轭)的. 数域 L 到复数域 $\mathbf{C}$ 的 $\mathbf{Q}$-嵌入也简称为嵌入.

定理1　设 K 为数域，L 为其 n 次扩张. 则 L 到复数域 $\mathbf{C}$ 恰有 n 个不同的 K-嵌入. 类似地，K 到 $\mathbf{C}$ 的每一个嵌入 σ 恰可延拓为 n 个 L 到 $\mathbf{C}$ 的不同嵌入 $\sigma_i(1 \leq i \leq n)$.

证明 只需证后一结论，再令 $\sigma=1$ 为恒等映射即得前一结论. 取 $\alpha\in L-K$，设 $f(X)$ 为其在 K 上极小(不可约)多项式，以 σ 作用于 f 的系数得多项式 σf，则 σf 在 σK 上不可约，应有 $m=\deg(f)$ 个互异复根，对每个复根 α_i 有 K-同构 $\sigma_i: K(\alpha)\to K(\alpha_i)$，$\alpha\longmapsto\alpha_i$. σ_i 是 σ 的延拓($1\leq i\leq m$). 而 σ 也只能有这 m 个延拓，因为每个延拓 τ 由 $\tau\alpha$ 唯一决定，而 $\tau\alpha$ 必为 σf 的某根 α_i. 由归纳法可设 $K(\alpha)$ 的每个同构 σ_i 到 L 有 $[L:K(\alpha)]$ 个延拓，故 σ 到 L 的延拓个数为 $[L:K(\alpha)]m=[L:K(\alpha)][K(\alpha):K]=[L:K]=n$. □

例 1 设 $K=\boldsymbol{Q}(\sqrt{m})$ 为二次域，则 K 到 C 有两个嵌入：

$$a+b\sqrt{m}\longmapsto a\pm b\sqrt{m}.$$

例 2 设 $K=\boldsymbol{Q}(\zeta_m)$ 为 m 级分圆域，则 K 到 $\boldsymbol{C}$ 有 $\varphi(m)$ 个嵌入：$\zeta_m\longmapsto\zeta_m^k$ (k 与 m 互素且小于 m).

设 L 为 $\boldsymbol{Q}$ 的 n 次扩张，σ 是 L 到 $\boldsymbol{C}$ 的嵌入. 若 $\sigma L\subset\boldsymbol{R}$，则称 σ 为**实嵌入**，否则称为**虚(复)嵌入**. 若 σ 是虚嵌入，则令 $\bar{\sigma}(\alpha)=\overline{\sigma(\alpha)}$ 可得共轭嵌入 $\bar{\sigma}$. 故可设共有 r_1 个实嵌入，$2r_2$ 个虚嵌入，$r_1+2r_2=n$.

定理 2 每个代数数域 K 均为 $\boldsymbol{Q}$ 的单扩张，即 $K=\boldsymbol{Q}(\alpha)$ (此 α 称为本原元素).

证明 设 $[K:\boldsymbol{Q}]=n$，由定理 1 知 K 到 $\boldsymbol{C}$ 有 n 个不同嵌入 σ_i ($1\leq i\leq n$). 我们将设法取 $\alpha\in K$ 使 $\sigma_i\alpha$ 彼此不同，于是 $\alpha=\sigma_1\alpha$

在 Q 上的极小多项式至少有 n 个互异根 $\sigma_i\alpha$，从而$[Q(\alpha):Q]\geq n$，即知 $K=Q(\alpha)$. 为此考虑方程 $\sigma_i(x)=\sigma_j(x)$，它的解 $x\in K$ 全体是 K 的一个子集 V_{ij}. 当 $i\neq j$ 时，V_{ij}是 K 的真子空间. 由线性代数内容可知，存在 $\alpha\in K$ 使 $\alpha\notin V_{ij}$对任意 $1\leq i,j\leq n$ 成立（例如，见[Zh22]第 75 页）. 这就证明了定理. □

注记（可分扩张） 设 L/K 为域的 n 次扩张，C 为 L 的代数闭包，σ 是 K 到 C 中的任一个嵌入. σ 到 L 上延拓的个数称为 L/K 的可分次数，记为$[L:K]_S$（不依赖于 σ 的选取）. 而$[L:K]_i=[L:K]/[L:K]_S$ 称为不可分次数. 若$[L:K]_S=n$ 则称 L/K 为**可分扩张**. 完全域 K 的任一代数扩张均为可分扩张（K 为**完全域**是指：K 的特征为 0；或者 $K^p=K$（K 的特征为 $n\neq 0$ 时））. 因此只有讨论有限域的超越扩张，即 $F_q(X)$的扩张时，才会遇到不可分扩张.

以上两定理对可分扩张也是成立的. 详言之，设 L/K 为 n 次可分扩张，则(1) L 到其代数闭包 C 有 n 个不同的 K-嵌入；(2)$L=K(\alpha)$对某 $\alpha\in L$ 成立. 前者包含在可分扩张的定义中，后者可类似于定理 2 证明.

对迹与范的概念，首先回忆线性代数. 设 V 是域 K 上 n 维线性空间，φ 是其线性变换. 取定 V 的基之后，φ 有方阵表示 $M=(a_{ij})$，$a_{ij}\in K$. 则定义 M 和 φ 的迹、范（或行列式）、特征多项式为：

$$\begin{aligned}
&\mathrm{Tr}(\varphi)=\mathrm{Tr}(M)=a_{11}+\cdots-a_{nn},\\
&N(\varphi)==\det(\varphi)=\det(M),\\
&f_\varphi(X)=f_M(X)=\det(XI-M)\\
&\qquad=X^n+\mathrm{Tr}(\varphi)X^{n-1}+\cdots+(-1)^nN(\varphi).
\end{aligned}$$

自然有 $\mathrm{Tr}(\varphi+\psi)=\mathrm{Tr}(\varphi)-\mathrm{Tr}(\psi)$，$N(\varphi\psi)=N(\varphi)N(\psi)$. 上述概念可稍作推广，设 V 是秩为 n 的自由 A-模(即 V 中每个元素可唯一地表为 $a_1\alpha_1+\cdots+a_n\alpha_n$，$a_i\in \mathrm{A}$)，A 为交换环，$\varphi$ 是其自同态，则仍有上述定义和结果.

定义 1 设 $A\subset B$ 均为含幺交换环，且 B 是秩为 n 的自由 A-模(例如 $A\subset B$ 均为数域). 于是每个 $\alpha\in B$ 定义了 B 的一个自同态

$$\varphi_\alpha: x \longrightarrow \alpha x.$$

则 φ_α 的迹、范(或行列式)、特征多项式分别称为 α 对于 B/A 的**迹**、**范**、和特征多项式，分别记为 $\mathrm{Tr}_{B/A}(\alpha)$，$N_{B/A}(\alpha)$，$f_{B/A,\alpha}(X)$，足标 B/A 也可省略.

显然对任意 $\alpha,\beta\in B$ 和 $\kappa\in A$ 均有 $\mathrm{Tr}(\alpha-\beta)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)$，$\mathrm{Tr}(\kappa\alpha)=\kappa\mathrm{Tr}(\alpha)$，$\mathrm{Tr}(\kappa)=n\kappa$；$N(\alpha\beta)=N(\alpha)N(\beta)$，$N(\kappa\alpha)=\kappa^nN(\alpha)$，$N(\kappa)=\kappa^n$.

定理 3 设 L/K 是数域的 m 次扩张，$\alpha\in L$ 在 K 上的极小多项式 $f(X)$ 的复根为 α_1，…，α_n(这即为 α 的 K-共轭元)，$d=[L:K(\alpha)]$. 则 α 对于 L/K 的迹、范、和特征多项分别为

$$\mathrm{Tr}(\alpha)=d(\alpha_1+\cdots+\alpha_n)=d\mathrm{Tr}_{K(\alpha)/K}(\alpha),$$
$$N(\alpha)=(\alpha_1\cdots\alpha_n)^d=(N_{K(\alpha)/K}(\alpha))^d,$$
$$f_\alpha(X)=((X-\alpha_1)\cdots(X-\alpha_n))^d=f(X)^d.$$

当 L/K 为任意 m 次可分扩张时，以上结论仍成立，此时 $\alpha_1,\cdots,\alpha_n$ 是 $f(X)$ 在 L 的一个代数闭包 C_L 中的根.

证明 首先设 $d=1$. 于是 $L=K(\alpha)\cong K[X]/(f(X))$，且 $1,\alpha,\cdots,\alpha^{n-1}$ 是 L 的 K-基. 设

$$f(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0=0\quad(a_{n-1},\cdots,a_0\in K),$$
则定义 I 中 φ_α 的方阵表示为 $f(X)$的友阵

$$M=\begin{pmatrix}0&\cdots&\cdots&0&-a_0\\1&\ddots&&\vdots&-a_1\\0&1&\ddots&\vdots&-a_2\\\vdots&\ddots&\ddots&0&\vdots\\0&\cdots&0&1&-a_{n-1}\end{pmatrix},$$

由此知 $f_\alpha(X)=\det(XI-M)=f(X)$，$\mathrm{Tr}(\alpha)=-a_{n-1}=\alpha_1+\cdots+\alpha_n$，$N(\alpha)=(-1)^{n-1}a_0=\alpha_1\cdots\alpha_n$.

再考虑一般情形. 此时 $1,\alpha,\cdots,\alpha^{n-1}$是 $K(\alpha)$的 K-基，设 $\beta_1,\cdots,\beta_d$ 是 L 的 $K(\alpha)$-基，则$\{\alpha^i\beta_j\}$是 L 的 K-基，故 φ_α 的方阵表示为

$$M_1==\begin{pmatrix}M&&\\&\ddots&\\&&M\end{pmatrix},$$

由此即得定理 1. □

定理 4 (1)设 L/K 为数域有限扩张，则 L 中整数 α 的迹、范、和特征多项式系数均是 K 中整数.

(2)设 L/K 为有限可分扩张，K 为整环 A 的分式域，$\alpha\in L$ 是 A 上整元素. 则 α 对于 L/K 的迹、范、和特征多项式系数均在 A 上是整的，且属于 K(特别若 A 是整闭的，则它们均属于 A).

证明 只需证后一断言. 定理 3 对此情形仍成立，故仅需证明 α 的 K-共轭元 $\alpha_1,\cdots,\alpha_n$ 均在 A 上是整的. 这是显然的，因为它们是 α 的极小多项式(A 上首一)的根. □

定理 5(链性)　设域 $K\subset L\subset M$,则对 $\alpha\in M$ 有

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha))=\mathrm{Tr}_{M/K}(\alpha),$$
$$N_{L/K}(N_{M/L}(\alpha))=N_{M/L}(\alpha).$$

证明　设 α 在 K 上的(首一)极小多项式为 $f(X)$,在 L 上作不可约因子分解:$f(X)=f_1\cdots f_m$.可设 α 在 L 上的极小多项式为 f_1.于是 $N_{M/L}(\alpha)$即为 f_1 的常数项的 d 次幂($d=[M:L(\alpha)]$),再对 L/K 取范即是各 f_i 常数项 d 次幂之积,即 $f(X)$ 的常数项的 d 次幂,恰为 α 对 M/K 的范.对迹类似可证.　□

习　题

1. 列出如下域到 $\boldsymbol{C}$ 中的嵌入:$K_1=\boldsymbol{Q}(\sqrt{d})$,$K_2=\boldsymbol{Q}(\zeta_m)$,$K_3=\boldsymbol{Q}(\sqrt[3]{2})$.那些嵌入是域的自同构?

2. 设 u 是数域 K 的单位(即 u 和 u^{-1}均为整数),证明 u 到 $\boldsymbol{Q}$ 的范为±1.证明这也是整数 u 为单位的充分条件.

3. 证明 $9+\sqrt{10}$在 $\boldsymbol{Z}[\sqrt{10}]$中不可约;$\sqrt{3}\notin\boldsymbol{Q}(\sqrt[4]{2})$.(提示:用范和迹)

§1.4　元素的判别式

首先回忆线性代数见([Zh22]).设 V 是域 K 上 n 维线性空间,g 是 V 上一非退化的双线性型(g 是非退化的定义为:不存在固定的非零 α_0 使 $g(\alpha_0,\beta)=0$ 对任意 β 成立).设 $e_1,\cdots,e_n$ 是 V 的基,则方阵 $G=(g(e_i,e_j))$称为 g 在上述基下的方阵(表示),于是 $g(\alpha,\beta)=x'Gy$ 对任意 $\alpha,\beta\in V$ 成立,这里 x,y 是 α,β

的坐标列，x' 表示 x 的转置. g 非退化相当于 $\det G\neq 0$.

对任意 $\alpha_1,\cdots,\alpha_n\in V$，方阵 $G(\alpha_1,\cdots,\alpha_n)=(g(\alpha_i,\alpha_j))$ 称为 Gram 方阵，其行列式称为 $\alpha_1,\cdots,\alpha_n$ 的**判别式**(Discriminant)：

$$\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)=\det(g(\alpha_i,\alpha_j)).$$

故 $G(e_1,\cdots,e_n)=G$，$\mathrm{Disc}(e_1,\cdots,e_n)=\det P\neq 0$. 设 α_j 在基 $\{e_j\}$ 下的坐标列为 $P_j=(p_{1j},\cdots,p_{nj})$，即对方阵 $P=(p_{ij})$ 有 $(\alpha_1,\cdots,\alpha_n)=(e_1,\cdots,e_n)P$. 因此 $\alpha_1,\cdots,\alpha_n$ 线性无关当且仅当 $\det P\neq 0$. 而

$$\begin{aligned}\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)&=\det(g(\alpha_i,\alpha_j))=\det((P'_iGP_j))\\&=\det(P'GP)=(\det G)\det P^2\\&=\mathrm{Disc}(e_1,\cdots,e_n))\det P^2.\end{aligned}$$

这说明

$$\alpha_1,\cdots,\alpha_n\text{ 线性无关}\Leftrightarrow\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)\neq 0.$$

注记 若 V 对内积 g 是欧几里得空间(即域 K 是实数域子域，且 g 是正定对称的)，$\{e_i\}$ 为标准正交基，则判别式 $\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)=\det P^2$ 恰为向量 $\alpha_1,\cdots,\alpha_n$ 所夹平行体的体积(测度) $\det P$ 的平方(因为 P 的各列是各向量 α_j 的坐标).

特别若取 $\alpha_1,\cdots,\alpha_n$ 为 $e_1,\cdots,e_n$ 的对偶基，即满足：$g(\alpha_i,e_j)=\delta_{ij}$，$\delta_{ij}=1$ 或 0(依 $i=j$ 与否). 则 $g(\alpha_i,\alpha_j)=g(\alpha_i,p_{1j}e_1+\cdots+p_{nj}e_n)=p_{ij}$. 故 $\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)=\det(p_{ij})=\det P$. 由于 $\{\alpha_i\}$ 到 $\{e_i\}$ 的过渡方阵为 P^{-1}，故 $\mathrm{Disc}(e_1,\cdots,e_n)=\det P^{-1}$，即知 $\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)=\mathrm{Disc}(e_1,\cdots,e_n)=1$.

现在转向讨论 L/K 为域的 n 次扩张，L 作为 K 上线性空间具有一个自然的对称双线性型(内积)

$$g(\alpha,\beta)=\mathrm{Tr}(\alpha\beta),$$

这里 Tr 表示对于 L/K 的迹. 若 K 为数域(或 L/K 是可分的)，

则 g 是非退化的;如果有固定的非零 α_0 使 $\mathrm{Tr}(\alpha_0\beta)=0$ 对任意 β 成立,则意味着 $\mathrm{Tr}(L)=0$,此不可能(例如见 S. Leng 所著 Algebra,第 211 页). 于是上述关于 V 和 $g(\alpha,\beta)$ 的一切均适用于 L 和 $\mathrm{Tr}(\alpha\beta)$. 以后总是以 $\mathrm{Tr}(\alpha\beta)$ 为扩域的内积. $\alpha_1,\cdots,\alpha_n\in L$ 对于 L/K 的判别式记为

$$\mathrm{Disc}_{L/K}(\alpha_1,\cdots,\alpha_n) \quad 或 \quad \mathrm{Disc}(\alpha_1,\cdots,\alpha_n) 或 \mathrm{D}(\alpha_1,\cdots,\alpha_n).$$

定理 1 设 L/K 为数域的(或可分的) n 次扩张,$\sigma_i(1\leq i\leq n)$ 是 L 的 K-共轭,$\alpha_1,\cdots,\alpha_n\in L$. 则

(i) $\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)=\det(\mathrm{Tr}(\alpha_i\alpha_j))=\det(\sigma_i\alpha_j)^2$.

(ii) 若 $L=K(\alpha)$,记 $\sigma_i\alpha=\alpha_i,\alpha_1=\alpha$,则 $1,\cdots,\alpha^{n-1}$ 的(也称为 α 的,或其极小多项式的)判别式

$$\mathrm{Disc}(1,\alpha,\cdots,\alpha^{n-1}) = \det(\alpha_i{}^j)^2 = \prod_{i<j}(\alpha_i-\alpha_j)^2$$

$$= \det\begin{pmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \cdots & \cdots & \cdots & \cdots \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{pmatrix} = (-1)^{n(n-1)/2} N_{L/K} f'(\alpha).$$

其中 $s_i=\alpha_1^i+\cdots+\alpha_n^i$,$f'(\alpha)$ 为 α 的极小多项式 $f(X)$ 的导数值. ($f'(\alpha)$ 称为 α 对 L/K 的差分)

证明 (i) 由如下的方阵恒等式即得:

$$(\sigma_i\alpha_j)^t(\sigma_i\alpha_j)=(\mathrm{Tr}(\alpha_i\alpha_j)).$$

(ii) 由 Vandermonde 行列式即知前三式相等. 计算出 $(\alpha_i^j)^t(\alpha_i^j)$ 则知其与第四式相等. 又由于

$$f(X)=(X-\alpha_1)\cdots(X-\alpha_n),$$

其导数值及其范为

$$f'(\alpha_i) = \prod_{\substack{j \\ i \neq j}} (\alpha_i - \alpha_j),$$

$$N_{L/K} f'(\alpha) = f'(\alpha_1) \cdots f'(\alpha_n) = \prod_{i \neq j} (\alpha_i - \alpha_j)$$

$$= \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

故知最后的等号成立. □

例 1 设 $f(X) = X^n + aX + b$ 为 $\alpha \in L$ 在 K 上的极小多项式. 于是 $f'(X) = nX^{n-1} + a$. 按上节方法, 考虑由 $f'(\alpha)$决定的 $K(\alpha)$上的线性交换 φ: $v \longmapsto f'(\alpha)v$. 由 $\varphi(1) = n\alpha^{n-1} + a$, $\varphi(\alpha) = (a - an)\alpha - b$ 等等, 易算得 φ 在基 $1, \cdots, \alpha^{n-1}$下的方阵表示为

$$M = \begin{pmatrix} a & -nb & & \\ & a-an & \ddots & \\ & & \ddots & -nb \\ n & & & a-an \end{pmatrix},$$

故 $N_{L/K} f'(\alpha) = \det M = a(a-an)^{n-1} + n^n b^{n-1}$, 即得

$$\mathrm{Disc}(1, \alpha, \cdots, \alpha^{n-1})$$
$$= (-1)^{n(n-1)/2}((-1)^{n-1} a^n (n-1)^{n-1} + n^n b^{n-1}).$$

特别 $n=2$ 时得 $X^2 + aX + b$ 的判别式为 $a^2 - 4b$. $n=3$ 时得 $X^3 + pX + q$ 的判别式为 $-(4p^3 + 27q^2)$.

§1.5 整基和域的判别式

设 L/K 为数域的 n 次扩张, 则 L 的整数环 O_L 是 O_K-模. 此模显然是无挠的(即 $a\alpha \neq 0$ 对任意非零的 $a \in O_K$ 和 $\alpha \in O_L$ 成立). 我们将证明 O_L 是一个自由 O_K-模 M 的子模. 注意, 若 A 为任一环, 那么"M 是秩为 n 的自由 A-模"的意义为: 存在 $\alpha_1, \cdots, \alpha_n \in M$ 使 M 中任意元素可唯一地表为 $a_1\alpha_1 + \cdots + a_n\alpha_n$. 此时也

记为 $M=A\alpha_1\oplus\cdots\oplus A\alpha_n$，而 $\alpha_1,\cdots,\alpha_n$ 称为 M 的 A-基.

定理 1 (i) 设 L/K 为数域的 n 次扩张. 则 O_L 是一个秩为 n 的自由 O_K-模的子模. 而当 O_K 是主理想环时(例如 $K=\boldsymbol{Q}$ 而 $O_K=\boldsymbol{Z}$ 时)，O_L 是秩为 n 的自由 O_K-模.

(ii) 设 L/K 是特征为 0 域的 n 次扩张，K 为环 A 的分式域且 A 是整闭的，B 是 A 在 L 中的整闭包(即在 A 上整的 L 中元素全体). 则 B 是一个秩为 n 的自由 A-模的子模. 若 A 是主理想环，则 B 是秩为 n 的自由 A-模.

证 只需证(ii)，(i)是其特例：$A=O_K$，$B=O_L$. 设 $\alpha_1,\cdots,\alpha_n$ 是 L 的 K-基，可设 α_i 均为 A 上整元素(否则乘以 A 上适当元素即可，见 §1.2). 设 $\beta_1,\cdots,\beta_n$ 是 $\alpha_1,\cdots,\alpha_n$ 的对偶 K-基，于是 $\mathrm{Tr}(\alpha_i\beta_j)=\delta_{ij}$. 任一 $\alpha\in B$ 可表为 $\alpha=a_1\beta_1+\cdots+a_n\beta_n$，$a_i\in K(1\leq i\leq n)$. 于是 $\mathrm{Tr}(\alpha_i\alpha)=a_i$，故 a_i 在 A 上是整的(§1.3)，从而 $a_i\in A(1\leq i\leq n)$，即 $\alpha\in A\beta_1\oplus\cdots\oplus A\beta_n$. 即知 B 是自由模 $M=A\beta_1\oplus\cdots\oplus A\beta_n$ 的子模. 当 A 为主理想环时，有事实"秩为 n 的自由 A-模 M 的子模均为自由模，且子模 B 的秩不超过 n". 在本定理情形下，B 的 A-基也是 L 的 K-基(因 L 中元素可表为 α/a，$\alpha\in B$，$a\in A$). 故 B 的秩(即 A-基的元素个数)为 n. □

对于定理 1(ii)中的扩张 L/K，若 B 是自由 A-模，即若 $B=A\alpha_1\oplus\cdots\oplus A\alpha_n$，则称 $\alpha_1,\cdots,\alpha_n$ 为 B 的 A-基，或 L/K 的**整基**(integral basis). 当 $K\neq\boldsymbol{Q}$ 时，数域扩张 L/K 的整基也称为**相对整基**，不一定存在. 如果扩张 L/K 有整基 $\alpha_1,\cdots,\alpha_n$，则定义 L/K 的**判别式**(理想)为其整基的判别式所生成的 A 的理想：

$$\mathrm{Disc}(L/K)=(\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)),$$

也记为 $D(L/K)$. 这一定义不依赖于整基的选取：设 $\beta_1,\cdots,\beta_n\in B$，则

$$(\beta_1,\cdots,\beta_n)=(\alpha_1,\cdots,\alpha_n)P,$$

方阵 P 的系数属于 A；于是由上节知

$$D(\beta_1,\cdots,\beta_n)=D(\alpha_1,\cdots,\alpha_n)(\det P)^2,$$

即任意 n 个整元素的判别式是整基判别式的平方倍. 若要 $\beta_1,\cdots,\beta_n$ 也为整基，它与 $\alpha_1,\cdots,\alpha_n$ 应能互相线性表出，故 P^{-1}的系数也属于 A(即 $\det P$ 为单位)；故不同整基的判别式相差一个单位的平方$(\det P)^2$ 倍，它们生成的理想是相等的. 特别当 $K=\boldsymbol{Q}$ 时，单位只有±1，故不同整基的判别式都是相等的，此时域的判别式 Disc(L/$\boldsymbol{Q}$)定义为任一整基的判别式，而不必再定义为它生成的理想. Disc($L/\boldsymbol{Q}$)常记为 Disc(L)或 $D(L)$，也称为 L 的**绝对判别式**. 我们已证明了如下定理 2.

定理 2 若扩张 L/K 有整基(即若 B 是自由 A-模)，则 $\beta_1,\cdots,\beta_n\in B$ 是 L/K 的整基的充分必要条件为$(D(\beta_1,\cdots,\beta_n))=D(L/K)$.

定理 3 (1) (Stickelberger 判则). 数域 L 的绝对判别式满足

$$D(L)\equiv 0 \text{ 或 } 1 \pmod 4.$$

(2) 数域 L 的绝对判别式 $D(L)$的符号为$(-1)^{r_2}$，即

$$D(L)==(-1)^{r_2}|D(L)|,$$

其中 $2r_2$ 为 L 到 $\boldsymbol{C}$ 的虚嵌入个数.

证 设 $\alpha_1,\cdots,\alpha_n$ 是 L 的绝对整基，则 $D(L)=(\det(\sigma_i\alpha_j))^2$ (σ_i 是L 到$\boldsymbol{C}$ 的$\boldsymbol{Q}$—嵌入)). (1)行列式$\det(\sigma_i\alpha_j)$是$n!$ 项之和，每项对应着$\{1,\cdots,n\}$的一排列. 记其中正号项(对应偶排列者)之和为 P，负号项(对应奇排列者)之和为 N，则 $D(L)=(P-N)^2=(P+N)^2$

$-4PN$，注意 $P-N$ 和 PN 在 σ_i 作用下均不变（σ_i 的作用相当于重排行列式各行次序，故 P,N 或不变或互变），从而均为有理整数，由此立得(1)。

(2) 注意

$$\overline{\det(\sigma_i\alpha_j)}=\det(\overline{\sigma_i\alpha_j})=\det(\overline{\sigma_i}(\alpha_j))=(-1)^{r_2}\det(\sigma_i\alpha_j).$$

最后一等号是因为复共轭变换恰对换了 r_2 行. 故依 r_2 为偶、奇数，$\det(\sigma_i\alpha_j)$ 为实、虚数，$D(L)$ 为正、负数. □

现在转向一般情形. 如果 L/K 没有相对整基，即 B 不是自由 A-模，需要引入如下定义.

定义 1 设 L/K 为域的 n 次扩张如定理 1，则其**判别式** $\mathrm{Disc}(L/K)$ 定义为所有 n-数组 $\alpha_1,\cdots,\alpha_n\in B$ 的判别式 $\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)$ 生成的 A 的理想，也记为 $D(L/K)$. (以后会看到，此定义等价于说 $D(L/K)$ 是所有理想 $(D(\alpha_1,\cdots,\alpha_n))$ 的最大公因子).

例 1 设 $K=\boldsymbol{Q}(\sqrt{m})$ 为二次域. 已知其整基为 $\{1,\sqrt{m}\}$ (当 $m\equiv 2$ 或 $3(\mathrm{mod}\,4)$)，或 $\{1,(1+\sqrt{m})/2\}$ (当 $m\equiv 1(\mathrm{mod}\,4)$) (§1.1). 在两情形下，易分别计算得其判别式为

$$\mathrm{Disc}(K)=4m \text{ 或 } m.$$

习 题

1. 求 $\boldsymbol{Q}(\sqrt{3},\sqrt{5})$，$\boldsymbol{Q}(\sqrt{2},\sqrt{3})$ 的判别式.

2. 求证 $f(X)=X^3-X-1$ 在 $\boldsymbol{Q}$ 上不可约. 设 α 为其一复根，$K=\boldsymbol{Q}(\alpha)$. 求 $D(1,\alpha,\alpha^2)$，并由此求 K 的整基. 对 $f(X)=X^3+10X+1$ 考虑同样的问题.

第二章 诺特环与戴德金环

数域的整数环中，理想可唯一分解为素理想之积. 这是代数数论的基础. 本章主要讨论这一理论. 历史上，人们在研究费尔马大定理和高次互反律时，遇到了复数不满足唯一因子分解律的困难. 最简单的例子是

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

容易看出 $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ 都是二次域 $\boldsymbol{Q}(\sqrt{-5})$ 整数环中的不可约元，互相也非结合元素(考虑元素的范即可知). 故这确是 6 的两种不同分解. Kummer 为了克服这一困难，发明了"理想数"的概念. 后经发展，建立了整数环及 Dedekind(戴德金)环中的理想唯一分解理论，奠定了代数数论的基础. Noether(诺特)环是稍广泛些的一类整环，在代数几何等领域非常重要.

§2.1 Noether 环

定理 1 (Noether 模) 设 A 为(含幺交换)环，M 是 A-模，则以下条件等价(满足条件之一的模 M 称为 **Noether 模**)：

(i)(极大条件)M 的每个非空子模族中均有极大元(即不含于此族中其它子模的子模).

(ii)（有限生成条件）M 的每个子模均是有限生成的.

(iii)（升链条件）M 中子模的每个升链均是稳定的（即对每个子模的序列 $M_1 \subset M_2 \subset M_3 \subset \cdots$，必存在 n 使 $M_n = M_{n+1} = M_{n+2} = \cdots$.）

证. (i)⇒(ii)：设 E 是 M 的子模，Ω 是 E 的所有有限生成的子模集合. 因零子模属于 Ω，故 Ω 非空. 由(i)知 Ω 有极大元，设为 F. 任取 $x \in E$，$F + Ax$ 也是有限生成的子模，故必有 $F + Ax = F$，即 $x \in F$. 因此 $E = F$，E 是有限生成的.

(ii)⇒(iii)：设 $M_1 \subset M_2 \subset M_3 \subset \cdots$ 是 M 的子模升链，则 $E = \bigcup_{n \geq 1} M_n$ 是 M 的子模，由(ii)知 E 是有限生成的，设它的有限个生成元 $x_1, \cdots, x_r$ 分别属于 $M_{n_1}, \cdots, M_{n_r}$，$n_1 \leq \cdots \leq n_r$. 于是当 $n \geq n_r$ 时总有 $M_n = M_{n_r} = E$.

(iii)⇒(i)：假定存在 M 的一个非空子模族 S 无极大元. 任取子模 $M_1 \in S$，则 S 中应有子模 M_2 包含 M_1 而不等于 M_1. 又因 S 中无极大元，故 S 中应有子模 M_3 包含 M_2 而不等于 M_2. 如此续行，则可得一无限升链，与(iii)矛盾. □

环 A 自身是一个 A-模，理想是此模的子模. 因此可用研究模的方法研究环和理想. 如果环 A 作为 A-模是 Noether 模，则称 A 为 **Noether 环**. 特别可知，环 A 为 Noether 环当且仅当以下等价条件之一成立：

(i)（极大条件）环 A 的每个非空理想族均有极大元.

(ii)（有限生成条件）环 A 的每个理想均是有限生成的.

(iii)（升链条件）环 A 的每个理想升链均是稳定的.

主理想环显然均是 Noether 环（由(iii)）.

定理 2 （1）设 M 是 A-模，E 是其一个子模. 则 M 为 Noether 模当且仅当 E 和 M/E 均为 Noether 模.

（2）有限个 Noether A-模的直和仍为 Noether 模.

（3）Noether 环 A 上有限生成的 A-模必是 Noether 模.

证 （1）$\Rightarrow$：E 的子模是 M 的子模的一部分，故由定理 1(i) 知 E 是 Noether 模. M/E 的子模格同构于 M 的含 E 的部分子模格，故知 M/E 为 Noether 模.

$\Leftarrow$：设 E 和 M/E 均为 Noether 模，$M_1 \subset M_2 \subset M_3 \subset \cdots$ 是 M 的子模升链. 于是有 E 的子模升链（$(M_1 \cap E) \subset (M_2 \cap E) \subset (M_3 \cap E) \subset \cdots$，及 M/E 的子模升链 $(M_1 \cap E)/E \subset (M_2 \cap E)/E \subset \cdots$. 由于 E 和 M/E 为 Noether 模，故存在 N 使当 $n > N$ 时有 $M_n \cap E = M_{n+1} \cap E$，$(M_n + E)/E = (M_{n+1} + E)/E$. 我们要证明 $M_n = M_{n+1}$. 任取 $x \in M_{n+1}$，显然存在 $y \in M_n$ 及 $e_1, e_2 \in E$ 使 $x + e_1 \equiv y + e_2 (\mathrm{mod} E)$，即 $x - y \in M_{n+1} \cap E = M_n \cap E$，故 $x \in M_n$，所以 $M_n = M_{n+1}$. 即知 M 是 Noether 模.

（2）$M_1 \oplus M_2$ 有子模 M_1 和商模 $(M_1 \oplus M_2)/M_1 \cong M_2$，故由 (1) 知 $M_1 \oplus M_2$ 为 Noether 模.

（3）设 M 是有限生成的 A-模，生成元为 $\alpha_1, \cdots, \alpha_n$，则 M 是自由模 $A \oplus \cdots \oplus A$（n 重）的商模（即同态 $(1, \cdots, 1) \longmapsto (\alpha_1, \cdots, \alpha_n)$ 的象），即得所欲证. □

定理 3 （1）任一数域 L 的整数环 O_L 是 Noether 环.

（2）设 L/K 是域的有限可分扩张，且 K 是整闭 Noether 环 A 的分式域，B 是 A 在 L 中的整闭包. 则 B 是有限生成的 A-模，也是 Noether 环.

证 只需证(2). 上章已证明 B 是一秩有限自由 A-模的子模，故 B 是有限生成 A-模，故 B 是 Noether A-模(因 A 是 Noether 环). 此外，B 的理想均是 B 的 A-子模，故它们满足极大条件(定理 1(i))，这说明 B 也是 Noether 环. □

除数域的整数环 O_L 外，另一类重要的 Noether 环是代数函数域的"整数环"，即在定理 3(2)中设 $K=F(X)$ 为域 F 上的有理式形式域(有理函数域)，L 为 K 的有限可分扩张. K 是 $A=F(X)$ 的分式域，A 在 L 中的整闭包 $B=O_L$ 称为 L 的整数(元)环，是一 Noether 环. 更一般地，(多元)多项式环 $F[X_1,\cdots,X_n]$ 及其商环均是 Noether 环，这是代数几何中很重要的环.

任意多自然数中必有极小者(这称为自然数集的良序性(按数值排序))，这是数学归纳法的理论根据. 而 Noether 模的任意子模族中必有极大元，这使得对于 Noether 模有"类似于归纳法"的方法.

习 题

1. 整数环 $\mathbf{Z}$ 是否满足降链条件(即每个理想降链都是稳定的)? 极小条件呢? $\boldsymbol{Q}[X_1,\cdots,X_n]$和 $\boldsymbol{Q}(X_1,\cdots,X_n)$又怎样?

§2.2 素理想与分式理想

设 A 为含幺交换环，$\wp$ 为其理想. 若商环 $A/\wp$ 是整环(即无零因子)，则称 $\wp$ 为素理想(prime ideal). 这相当于集合 $A-\wp$ 对乘法封闭：若 A 中 $x,y\notin\wp$ 则积 $xy\notin\wp$ (即 $xy\not\equiv 0 \pmod{\wp}$). 极大理想均是素理想，反之不真.

设环 $B\supset A$，$\mathfrak{q}$ 是 B 的素理想，则

$$\wp = \mathfrak{q} \cap A$$

是 A 的素理想. 事实上显然有 $A/\wp \subset B/\mathfrak{q}$(或者说 $a+\wp \longmapsto a+\mathfrak{q}$ 为单射:$A/\wp \to B/\mathfrak{q}$),故 $A/\wp$ 是整环,即知 $\wp$ 是素理想. $\wp$ 称为**位于 $\mathfrak{q}$ 下**的素理想;$\mathfrak{q}$ 称为**位于 $\wp$ 上**的素理想,$\mathfrak{q}$ 也称为 $\wp$ 的(素理想)因子. 此时 $\wp$(的元素)在 B 中生成的理想 $\wp B$ 显然含于 $\mathfrak{q}$ 中,即

$$\wp B \subset \mathfrak{q}, \qquad \text{或} \qquad \mathfrak{q} \mid \wp B.$$

定义 1. 设 I,J 为环 A 的理想.

(1)理想的乘积 IJ 定义为其元素的乘积所生成的理想,即由集合 $\{xy \mid x\in I, y\in J\}$ 生成的理想.

(2) 设 E 是 A-模,则定义 IE 为元素集 $\{xy \mid x\in I, y\in E\}$ 生成的 A-模.

(3) 若 $I\supset J$ 则记为 $I \mid J$,称 I 是 J 的因子,J 是 I 的倍,或 I 能整除 J.

例如对 $A=\mathbf{Z}, I=(4)=4\mathbf{Z}, J=(6)$,则 $(4)(6)=(24)$. 而 $(4)\cap(6)=(12)$. 故 $(4)(6)\subset(4)\cap(6)$. 一般地有 $IJ\subset I\cap J$. 所以在比较理想时,有两种序:包含关系和因子关系,二者正好相反.

引理 1 若 $\wp \supset I_1I_2\cdots I_n$,则存在 i 使 $\wp \supset I_i(1\leqslant i\leqslant n)$,这里 $\wp$ 为环 A 的素理想,$I_1,\cdots,I_n$ 为 A 的理想.(此引理也可叙述为:若 $\wp \mid I_1\cdots I_n$,则 $\wp \mid$ 某 I_i.)

证明 若对每个 i 均有 $\wp \not\supset I_i$,则 I_i 中有元素 $a_i \notin \wp$,于是 $a_1\cdots a_n \notin \wp$. 与 $a_1\cdots a_n\in I_1\cdots I_n\subset \wp$ 矛盾. □

引理 2 在 Noether 环 A 中，每个理想 I 都包含一些素理想的乘积．在 Noether 整环 A 中，每个理想 I 都包含一些非 0 素理想的乘积．

证明 只需对 A 为 Noether 整环的情形证明，另一情形的证明类似，只需去掉"非 0"字样．我们使用 Noether 环论中常用的类似归纳法的方法：

1）对 $I=A$ 引理显然成立，即 A 是零个素理想的乘积．

2）假设 J 为任一理想，且引理对满足 $I|J, I\neq J$ 的所有理想 I 成立，可证引理对 J 也成立．事实上，若 J 为素理想或 A，则引理显然成立．否则，A 中有元素 $x, y\notin J$ 而 $xy\in J$．于是 $J+Ax\supsetneqq J, J+Ay\supsetneqq J$，即 $(J+Ax)|J$，$(J+Ay)|J$，按上述(归纳)假设可知引理对 $J+Ax$ 和 $J+Ay$ 均成立，故有素理想 $\wp_i$ 使

$$J+Ax\supset\wp_1\cdots\wp_s,\qquad J+Ay\supset\wp_{s+1}\cdots\wp_t$$

故由 $xy\in J$ 知 $J\supset(J+Ax)(J+Ay)\supset\wp_1\cdots\wp_s\wp_{s+1}\cdots\wp_t$.

上述过程已证明了引理：若引理不真，则不满足引理的理想族中必有极大元(因 A 为 Noether 环)，设为 J．于是引理对所有满足 $I\supset J$(即 $I|J$)和 $I\neq J$ 的 I 成立，由(2)即知引理对 J 也成立，与 J 的定义矛盾． □

定义 2 设 K 为整环 A 的分式域，I 是 K 的 A-子模，并且有非 0 元 $d\in A$ 使 $dI\subset A$，则称 I 是 A 的(或 K 对 A 的)**分式理想**，也称为理想．(而 A 的普通理想有时被称为**整理想**，以作区别)．

所以，分式理想就是有着公分母 d 的 K 的子模．特别整理

想也是分式理想($d=1$). 例如,$\frac{2}{3}\mathbf{Z}=\left\{\frac{2}{3}k\mid k\in\mathbf{Z}\right\}$是 $\mathbf{Z}$ 的分式理想.

引理 3 设 A 为 Noether 整环,K 为其分式域. 则 K 的有限生成的 A-子模即为 A 的分式理想,反之亦真.

证明 设 $\alpha_1\cdots\alpha_n$ 是 K 的子模 M 的生成元,则这些 α_i 有"公分母"d(设 $d_i\alpha_i\in A,d_i\in A$,则令 $d=d_1\cdots d_n$ 即可),易知 $dM\subset A$,故 M 是分式理想. 反之,若 I 是 A 的分式理想,由于 A 是 Noether 环,作为 A-模 I 必是有限生成的(这是由于 $I\subset d^{-1}A$,后者作为 A-模与 A 同构,故是 Noether 模). □

分式理想 I 与 J 的积 IJ 定义为集合 $\{xy\mid x\in I,y\in J\}$所生成的 A-模,恰为有限和 $\sum_i x_iy_i(x_i\in I,y_i\in J)$全体. 显然分式理想 I 与 J 的交 $I\cap J$,和 $I+J$,积 IJ 均仍为分式理想. A 的非 0 分式理想全体是含 1($=A$)半群.

在此叙述中国剩余定理,它对一般环均适用,以便于以后应用,定理的形式和证明均与初等数论中的相应定理(孙子定理)类似.

定理 1 (中国剩余定理) 设 A 为一含幺交换环,$I_1,\cdots,I_n$ 为其两两互素的理想(即 $I_i+I_j=A$ 对所有 $i\neq j$). 任给 $x_1,\cdots,x_n\in A$,则存在 $x\in A$ 使 $x\equiv x_i(\mathrm{mod}\ I_i)$对所有 i 成立.

证明 先看 $n=2$ 情形,由 $I_1+I_2=A$ 知 $a_1+a_2=1$ 对某 $a_1\in I_1$, $a_2\in I_2$ 成立. 于是令 $x=x_2a_1+x_1a_2$ 即可.

对一般的 n，我们先证明 $I_2\cdots I_n$ 与 I_1 互素．事实上对每个 i 可取 $a_i\in I_1$，$b_i\in I_i$ 使

$$a_i + b_i = 1 \qquad (i \geqslant 2)$$

于是

$$1=(a_2+b_2)\cdots(a_n+b_n)\in I_1+I_2\cdots I_n$$

（因除 $b_2\cdots b_n\in I_2\cdots I_n$ 一项外，其余项均 $\in I_1$）. 故可像 $n=2$ 情形一样取得 $y_1\in A$ 使

$$\begin{cases} y_1 \equiv 1 \pmod{I_1} \\ y_1 \equiv 0 \pmod{I_2\cdots I_n} \end{cases}$$

同样可得 $y_2,\cdots,y_n$ 使

$$\begin{cases} y_j \equiv 1 \pmod{I_j} \\ y_j \equiv 0 \pmod{I_i}(i \neq j) \end{cases}$$

再令 $x=x_1y_1+\cdots+x_ny_n$ 即可． □

习　题

1　若环 A 的理想 $I_1,\cdots,I_n$ 两两互素，则 $I_1I_2\cdots I_n=I_1\cap I_2\cdots\cap I_n$（提示：归纳法）.

2　设如定理 1，证明若 $I_1\cap\cdots\cap I_n=\{0\}$ 则定理中的 x 唯一存在.

§2.3　Dedekind 环

若环 A 的非零素理想均为极大理想，则称 A 的**维数**是 1.

定义 1　一维整闭 Noether 整环称为 Dedekind 整环．

例如，主理想环均是 Dedekind 环，但唯一析因环不一定是 Dedekind 环，因为不一定是一维的，例如多元多项式环．

定理 1 (1) 数域 L 的整数环是 Dedekind 环．

(2) 设 L/K 是域的有限可分扩张，K 是 Dedekind 环 A 的分式域，B 是 A 在 L 的整闭包，则 B 是 Dedekind 环．

证明 只需先证(2)，令 $A=\mathbf{Z}$ 即得(1)．我们已知 B 是整闭 Noether 整环，只需再证其维数为 1．为此取 B 的任一非 0 素理想 $\mathfrak{q}$，令 $\wp=\mathfrak{q}\cap A$．我们先证 $\wp$ 为 A 的极大理想，即 $A/\wp$ 是域，再由 $B/\mathfrak{q}$ 在 $A/\wp$ 上整(因 B 在 A 上整)，即可知 $B/\mathfrak{q}$ 是域，即得 $\mathfrak{q}$ 是极大理想．在 § 2.2 已证 $\wp$ 是 A 的素理想，现在只需再证 $\wp\neq(0)$，则由 A 是 Dedekind 环便可知 $\wp$ 是极大理想，任取非 0 元 $\alpha\in\mathfrak{q}$，其范即是 $\wp$ 中非 0 元，事实上，设 α 满足的最低次的整性方程为

$$\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0. \qquad (a_i\in A)$$

于是知 $a_0\neq 0$(否则消去 α 可降低方程次数)，由上式即知

$$\begin{aligned}0\neq a_0&=(-\alpha^{n-1}-a_{n-1}\alpha^{n-2}-\cdots-a_1)\alpha\\&\in(B\alpha)\cap A\subset\mathfrak{q}\cap A=\wp.\end{aligned}$$

这就证明了定理． □

由定理 1 可知，可分代数函数域 L(即 $K=F(X)$的有限可分扩张，见 § 2.1)的整数环 O_L 是 Dedekind 环．在代数几何(或交换代数)中容易证明：光滑平面曲线 V 的坐标环 $R=C[V]$是 Dedekind 环．事实上，光滑曲线上的函数域(即坐标环的分式域)理论，与上述一元可分代数函数域的理论是相互对应的．

定理 2 Dedekind 环 A 中每个非 0 素理想 $\wp$ 均是可逆的(在其分式理想半群中)．也就是说，存在分式理想 $\wp^{-1}$ 使 $\wp^{-1}\wp$

$=(1)=A$.

证明 设$\wp$为Dedekind 环A的非0素理想. 令K为A的分式域而

$$\wp'=\{x\in K \mid x\wp\subset A\}.$$

则$\wp'$显然为A的分式理想($\wp$中任一元均可作其公分母),我们要证明$\wp'$是$\wp$的逆,即$\wp'\wp=(1)=A$. 首先显然有$\wp'\wp\subset A$. 而由于$A\subset\wp'$(因$\wp$为整理想),故$\wp=A\wp\subset\wp'\wp\subset A$,由于$\wp$为极大理想,故$\wp'\wp=A$或$\wp'\wp=\wp$.

只需再证$\wp'\wp\neq\wp$. 若$\wp'\wp=\wp$,任取$\alpha\in\wp'$则$\alpha\wp\in\wp$,从而$\alpha^2\wp\in\alpha\wp\in\wp$,由此可知$\alpha^n\wp\in\wp$对任意$n$成立($n$为自然数). 从而可知$A[\alpha]$是$A$的分式理想($\wp$中任一非0元为公分母). 但因$A$是Noether 环,故分式理想$A[\alpha]$是有限生成$A$-子模(上节引理3),从而$\alpha$在$A$上整(整性判则),故$\alpha\in A$. (因$A$整闭),即得$\wp'\subset A$,即$\wp'=A$. 下面证此不可能。

取非0元$a\in\wp$,则$\wp\supset(a)=A(a)\supset\wp_1\cdots\wp_n$(见上节引理2,$\wp_i$为非0素理想),取$n$为最小可能值. 于是$\wp\supset\wp_i$对某$i$成立. 不妨设$i=1$,又由于$\wp$和$\wp_1$均为极大理想(因$A$是Dedekind 环),故$\wp=\wp_1$. 记$\mathscr{C}=\wp_2\cdots\wp_n$,则$Aa\not\supset\mathscr{C}$(由$n$的最小性),故存在$b\in\mathscr{C}$使

$$b\notin Aa,\quad a^{-1}b\notin A$$

而
$$\wp b\subset\wp\mathscr{C}=\wp_1\wp_2\cdots\wp_n\subset Aa$$

即
$$a^{-1}b\wp\subset A,\ a^{-1}b\in\wp'(\text{由}\wp'\text{的定义})$$

即知$\wp'\neq A$. □

定理3 设A是Dedekind 环,$\boldsymbol{P}$是A的非零素理想集,则

(i) A的每个非0分式理想I可唯一分解为素理想及其逆的积:

$$I = \prod_{\wp \in P} \wp^{n_\wp}$$

其中 $n_\wp = n_\wp(I) \in \mathbf{Z}$ 且只有有限个非 0，$\wp$ 过 A 的非 0 素理想．

(ii) A 的非 0 分式理想全体是群．

证明 (i) 先证分解的存在性，只需对整理想 I 证明，因为对每个分式理想 I 均有 A 的非 0 元 d 使 $dI \subset A$ 为整理想，而 $I = (dI)(Ad)^{-1}$. 我们使用类似归纳法的方法：

(1) $I = A$ 时定理成立($n_\wp$ 均为 0).

(2) 设 J 为任一理想，当 $I|J$ 且 $I \neq J$ 时，定理对 I 总成立，我们要证明定理对 J 成立．当 $J = A$ 时显然．当 $J \neq A$ 时，J 含于某极大理想 $\wp$ 中，即 $\wp|J$. 于是 $\wp^{-1}$ 是 A 的分式理想，而且有 $\wp^{-1}J|J$(由 $\wp^{-1} \supset A$ 知 $\wp^{-1}J \supset AJ = J$)，及 $\wp^{-1}J \neq J$(否则对 $\alpha \in \wp^{-1}$ 有 $\alpha J \subset J$，从而 $\alpha^n J \subset J$ 对任意 n 成立，从而 $A[\alpha]$ 是 A 的分式理想(J 的任一元可作公分母)，从而是有限生成 A-子模，即知 α 在 A 上整，于是 $\alpha \in A$，$\wp' \subset A$，即 $\wp' = A$. 这导致矛盾，(见定理 2 证明)). 故知

$$\wp^{-1}J = \wp_1 \wp_2 \cdots \wp_s,$$

$$J = \wp \wp_1 \wp_2 \cdots \wp_s.$$

上述步骤就证明了存在性：若不然，不能写为素理想之积的理想族有极大元，设为 J，则对 $I|J, I \neq J$ 的 I 存在性均成立，由上述(2)即知对 J 也成立，矛盾．

再证(i)的唯一性．若 I 有两种分解，将指数 $n_\wp$ 为正、为负的因子分开，则导致如下形式的等式：

$$\wp_1^{n_1} \cdots \wp_r^{n_r} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_s^{e_s}$$

其中 $\wp_i, \mathfrak{q}_i$ 为 A 的非 0 素理想，n_i, e_i 为正整数，且 $\wp_i \neq \mathfrak{q}_j$(对任意 i, j). 于是 $\wp_1 | \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_s^{e_s}$(即($\wp_1 \supset \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_s^{e_s}$)，故 $\wp_1$|某 $\mathfrak{q}_i$，(引

理 1)，设$\wp_1 | \mathfrak{q}_1$，即$\wp_1 \supset \mathfrak{q}_1$，但二者均为极大理想，故$\wp_1 = \mathfrak{q}_1$，矛盾．

(ii) 由(i)可知$\prod \wp^{-n_\wp}$显然是I的逆. □

习　题

1. 证明$\boldsymbol{Q}[X,Y]$，$\boldsymbol{Q}[X^2,X^3]$均非 Dedekind 环(后者显然是 Noether 环，前者也是．有著名的 Hilbert 基定理：若R为 Noether 环，则$R[X]$也是 Noether 环)．

§ 2.4　理想与理想类

以$\boldsymbol{I}(A)$记 Dedekind 环A的非 0 分式理想全体，上节定理 3 可简述为：(i) $\boldsymbol{I}(A)$中有"理想的唯一分解律"；(ii) $\boldsymbol{I}(A)$为乘法群. 可以证明，对于整环A以下三者等价：

A为 Dedekind 环$\Leftrightarrow \boldsymbol{I}(A)$有"理想唯一分解律"$\Leftrightarrow \boldsymbol{I}(A)$是乘法群．

现设K为 Dedekind 环A的分式域．K中每个元素α生成一个主分式理想$(\alpha) = A\alpha$，全体主分式理想记为$\mathscr{P}(A)$，这是$\boldsymbol{I}(A)$的一个子群，商群

$$H(K) = \boldsymbol{I}(A)/\mathscr{P}(A)$$

称为K的**理想类群**(Ideal Class Group)．理想类群的阶

$$h(K) = \# H(K)$$

称为K(或A)的**理想类数**，类群的每个元素(陪集)称为一个**理想类**. 显然两个分式理想I与J同类(或称等价)当且仅当

$$I \equiv J \pmod{\mathscr{P}(A)}$$

即
$$I = (\alpha)J = \alpha J$$

对某$\alpha \in K$成立．当I与J均为整理想时，可乘以α的分母而

把上式写为

$$\alpha_1 I = \alpha_2 J$$

对某二元素 $\alpha_1,\alpha_2\in A$ 成立.(附记,有时也定义其它等价,如当 K 为二次域时,I 与 J 的等价加限制条件 $N(\alpha_1\alpha_2)>0$,称为严义等价,将在§7.3.1介绍).

显然,A 为主理想环$\Leftrightarrow I(A)=\mathscr{P}(A)\Leftrightarrow h(K)=1$. 所以类数$h(K)$是 A 与主理想环差距的度量.

系 1 记号如上节定理 3,有以下结论成立:

(1) I 为整理想$\Leftrightarrow n_\wp(I)\geqslant 0$ (对任意 $\wp$).

(2) $I|J\Leftrightarrow n_\wp(I)\leqslant n_\wp(J)$ (对任意 $\wp$).

(3) $I+J=\prod\limits_{\wp}\wp^{\min\{n_\wp(I),n_\wp(J)\}}$,

(记 $I+J=\gcd\{I,J\}=(I,J)$).

(4) $I\cap J=\prod\limits_{\wp}\wp^{\max\{n_\wp(I),n_\wp(J)\}}$,

(记 $I\cap J=\operatorname{lcm}\{I,J\}$).

上述(2)进一步说明记号 $I|J$ 和 $\mathbf{Z}$ 中的整除记号 $a|b$ 类似,而不只是 $I\supset J$ 的另一种形式上的写法了.

证明 (1) 充分性显然,必要性由定理 3 证明过程即知,事实上正是对整理想证明的.

(2) 由 $I|J\Leftrightarrow I^{-1}J\subset A$ 即知.

(3) $I+J$ 是 I 和 J 对于包含关系的最小上界(即理想的"最大公因子"),由(2)即得.

(4) $I\cap J$ 是 I 和 J 对于包含关系的最大下界(即理想的"最小公倍数"),由(2)即得. □

系 2 设 $\mathscr{C}$ 是 Dedekind 环 A 的一个理想类，对于任一指定的整理想 J，类 $\mathscr{C}$ 中必含有与 J 互素的整理想 I. 特别每个理想类中必含整理想.

证明 任取 $\mathscr{C}$ 中一理想 C，其逆记为 C'，由以下可知，不妨设 C' 是整理想. 设 $C'J$ 中素理想因子全体为 $\wp_1 \cdots \wp_r$, $C' = \prod_{i=1}^{r} \wp_i^{e_i}$, $(e_i \geqslant 0)$，对每个 i，存在 A 中元 $\alpha_i \in \wp_i^{e_i} - \wp_i^{e_i+1}$（因为由分解的唯一性有 $\wp_i^{e_i} \supsetneqq \wp_i^{e_i+1}$），故有 A 中元 α 使

$$\alpha \equiv \alpha_i (\bmod\ \wp_i^{e_i+1}). \quad (1 \leqslant i \leqslant r)(\text{中国剩余定理})$$

由此可知 $\wp_i^{e_i} \| (\alpha)$ $(1 \leqslant i \leqslant r)$（这是由于 $(\alpha)+(\alpha_i) = A\alpha - A\alpha_i = A(\alpha - \alpha_i) \subset \wp_i^{e_i+1}$，而 $(\alpha_i) \subset \wp_i^{e_i}$, $(\alpha_i) \not\subset \wp_i^{e_i+1}$）. 于是 $(\alpha) = C'Q$，Q 不含素因子 $\wp_1, \cdots, \wp_r$. 即知 $\mathscr{C}$ 中含理想 $I = (\alpha)C = C'QC = Q$，与 J 互素. □

系 3 Dedekind 环 A 中任一理想 I 可由两个元素生成：$I = (\alpha, \beta)$，且其中一个元素 α 可在 I 中先任意选取.

证明 任取 $\alpha \in I$ 则 $I | (\alpha)$，故可设 $I = \prod_{i=1}^{r} \wp_i^{e_i}$, $(\alpha) = \prod_{i=1}^{r} \wp_i^{f_i}$, $0 \leqslant e_i \leqslant f_i (1 \leqslant i \leqslant r)$. 取 $\beta_i \in \wp_i^{e_i} - \wp_i^{e_i+1}$, $\beta \equiv \beta_i (\bmod\ \wp_i^{e_i+1}) (1 \leqslant i \leqslant r)$ 即可. 事实上，若记 $(\beta) = \prod \wp_i^{g_i}$，则 $(\alpha, \beta) = (\alpha) + (\beta) = \prod \wp_i^{d_i}$，其中

$$d_i = \min(f_i, g_i) = e_i \quad (1 \leqslant i \leqslant r).$$ □

系 4 设 A 是 Dedekind 环，则 A 为主理想环 $\Leftrightarrow$ A 为唯一析

因环.

证明 设 A 为唯一析因环,我们来证明其每个素理想 $\wp$ 均为主理想即可,由系 2 知存在整理想 I(即 $\wp^{-1}$所在类中的任一整理想)使

$$I\wp=(a)=(p_1\cdots p_r)=(p_1)\cdots(p_r),$$

其中(p_i)是由素元素 p_i 生成的理想,故为素理想. 由分解唯一性可知存在 i 使 $\wp=(p_i)$. □

证明 II 只需证(⇐). A 的任一理想 I 是有限生成的,设 $I=A\alpha_1+\cdots+A\alpha_n$,令

$$d=\gcd(\alpha_1,\cdots,\alpha_n),$$

则 $I=Ad$. 事实上,设 $\alpha_i=\prod_j p_{ij}^{e_{ij}}$,则$(\alpha_i)=\prod_j(p_{ij})^{e_{ij}}$,故由系(1)知

$$\begin{aligned}I&=(\alpha_1)+\cdots+(\alpha_n)\\&=\prod_j(p_{ij})^{\min_j(e_{ij})}=\prod_j(p_{ij}^{\min_j e_{ij}})=(d).\end{aligned}$$ □

习 题

1. $\boldsymbol{C}$ 中代数整数全体 $\boldsymbol{D}$ 是否 Dedekind 环?

§2.5 数论中的整环

对于代数数论中常用的环的类型及相互关系,现较系统地作介绍.

定义 1 （欧几里得环） 设 R 是含幺交换环，若存在 R 到 N（非负整数集，或任一良序集）的一个映射 φ 满足如下条件：

（E） 对任意的 $a,b\in R$，$b\neq 0$，必存在 $q,r\in R$ 使

$$a = bq + r, \text{且 } \varphi(r) < \varphi(b);$$

则称 R 为**欧几里得环**，称 φ 为**欧几里得映射**．

例如，当 $R=\mathbf{Z}$ 时，令 $\varphi(a)=|a|$，则可知 $\mathbf{Z}$ 是欧几里得环．当 $R=F[X]$为域 F 上多项式（形式）环时，令 $\varphi(a)=2^{\deg(a)}$，则 $F[X]$是欧几里得环（其中 $\deg(a)$为 a 的次数）．

注记 许多文献中关于欧几里得环的定义还附加其余的条件（例如 $\varphi(ab)\geqslant\varphi(a)$，$R$ 为整环等），事实上都是不必要的．

命题 1 欧几里得环 R 是主理想环．

证明 设 I 是 R 的非 0 理想，取非 0 元 $b\in I$ 使 $\varphi(b)$为最小可能值．于是对任意 $a\in I$，有 $a=bq+r$，且 $\varphi(r)<\varphi(b)$，因 $r=a-bq\in I$，故必然有 $r=0$，即知 $I=bR$． □

对欧几里得环 R，$\varphi(0)$必是 $\varphi(R)$的最小值，且当 $0\neq b\in R$ 时，$\varphi(b)>\varphi(0)$．事实上，由条件（E）可写 $0=bq+b_1$，$\varphi(b_1)<\varphi(b)$．若 $b_1\neq 0$ 则可写 $0=b_1q_1+b_2$，$\varphi(b_2)<\varphi(b_1)$．如此下去可得序列 $b,b_1,b_2,\cdots$，因为 N 中序列 $\varphi(b)>\varphi(b_1)>\varphi(b_2)>\cdots$是严格递降的，故必然是有限的，即存在 $n\geqslant 1$ 使 $b_n=0$．故 $\varphi(0)=\varphi(b_n)<\varphi(b)$．

除 $\varphi(0)$之外，若 $\varphi(b)$最小，则 b 必为 R 的单位．这是因为对任意 $a\in R$ 有 $a=bq+r$，$\varphi(r)<\varphi(b)$，故 $r=0$，即知 $R=bR$，b 为单位．例如 $\mathbf{Z}$ 中除 0 外，$|\pm 1|$最小．

命题 2 若 R 是主理想环且只有有限个极大理想，则 R 是欧几里得环．

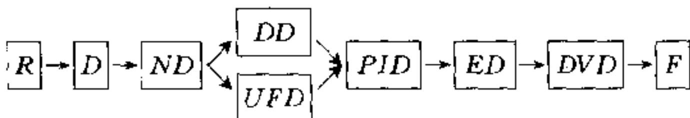
证明 设 $p_1,\cdots,p_s$ 生成 R 的全部极大理想 $(p_1),\cdots(p_s)$. 对任意非 0 元 $a\in R$，总是以同名字母 $a_1,\cdots,a_s$ 记 $a=p_1^{a_1}\cdots p_s^{a_s}$. 令映射 $\varphi: R\to \mathbf{N}$ 为

$$\varphi(a) = 1 + a_1 + \cdots + a_s, \qquad \varphi(0) = 0.$$

任给 $a,b\in R,b\neq 0$，(1)若 $b|a$ 则取 $r=0$. (2)若 $b\nmid a$ 则存在 $1\leqslant i\leqslant s$ 使 $a_i<b_i$. 若所有 $i=1,\cdots,s$ 均如此，则取 $r=a$；否则当 $a_j\geqslant b_j$ 时取 R 中元 $q_j\equiv a/b(\mathrm{mod}\ p_j)$，即 $a\equiv bq_j(\mathrm{mod}\, p^{1+b_j})$. 由孙子定理知存在 q 使 $q\equiv q_j-1(\mathrm{mod}\ p_j)$对所有这种 j 成立．令 $r=a-bq$，则 $r\equiv b(\mathrm{mod}\ p_j^{1+b_j})$，故 $r_j=b_j$. 即知 $\varphi(r)=1+r_1+\cdots+r_s<1+b_1+\cdots+b_s=\varphi(b)$，故 R 为欧几里得环． □

还可证明两个欧几里得环的直积也是欧几里得环；欧几里得环的分式环仍为欧几里得环．

环的进化图



以下作解释并举例，对每种环举出的例子均不属于高一级的环．

R(环)：n 阶全方阵环；$\mathbf{Z}/6\mathbf{Z}$.

D(整环)：代数数环 $((\sqrt[2^n]{2})$ 是其理想的无限升链)．

ND(Noether 整环)：$O_K[X_1,\cdots,X_n]$(其中 O_K 是数域 K 的整数环，$h(K)\neq 1$)；奇异曲线 V 的坐标环 $\boldsymbol{C}[V]$(例如 V 为 $Y^2=X^3$)．

DD(Dedekind 整环)：O_K(例如 $K=\boldsymbol{Q}(\sqrt{-5})$，$h(K)\neq 1$)；光滑曲线 V 的坐标环 $\boldsymbol{C}[V]$(当理想类数为 1 时是 PID)．

UFD(唯一析因整环)：$\mathbf{Z}[X_1,\cdots X_n]$

PID(主理想整环)：$\boldsymbol{Q}(\sqrt{d})$的整数环，其中 $d=-19,-43,-67,-163$. 例如 $\mathbf{Z}+\mathbf{Z}(1+\sqrt{-19})/2$.

ED(欧几里得整环)：$\boldsymbol{Z}$，$F[X]$，$\boldsymbol{Q}(\sqrt{d})$的整数环，其中 $d=-1,-2,-3,-7,-11,2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73$.

DVD(离散赋值环)：$(\mathbf{Z}-(p))^{-1}\mathbf{Z}$ ($\mathbf{Z}$ 对素理想(p)的局部化)；$\boldsymbol{Z}_p$ ($\boldsymbol{Z}$ 对 p—adic 赋值的完备化)；$F[[X]]$(形式幂级数环)；$\boldsymbol{C}[V]_P$(曲线在光滑点 P 的局部环)．

F(域)：$\boldsymbol{Q}$，$\boldsymbol{F}_p$，$\boldsymbol{Q}(X)$，$\boldsymbol{F}_p(X)$.

从 ND 开始，理想可分解为准素理想之交(I 称为准素理想是指：若 $xy\in I,x\notin I$,则 $y^m\in I$ 对某 $m>0$ 成立)．对一维 ND，上述准素分解是唯一的．UFD 只能是 PID 上的(多元)多项式环(Kantz 定理)．从 UFD 开始，素元(不可约元)生成的理想必是素理想．从 DD 开始，非 0 素理想必是极大理想(一维)．从 PID 开始有 Bezout 等式(即 a,b 的公因子可表为 $d=sa+tb$)．$\boldsymbol{Q}(\sqrt{-19})$等的整数环不是欧几里得环的证明见§7.2.

注记 1　关于 Noether 环的例子，若 V 是奇异曲线，则

$\boldsymbol{C}[V]$不再是整闭的，故 $\boldsymbol{C}[V]$不是 Dedekind 环，也不是 UFD. 而 $\boldsymbol{C}[V]$是 $\boldsymbol{C}[X,Y]$的商环，故是 ND. 例如，对 $V: Y^2-X^3=0$，我们有

$$R=\boldsymbol{C}[V]=\boldsymbol{C}[X,Y]/(Y^2-X^3)=\boldsymbol{C}[x,y]=\boldsymbol{C}[x,\sqrt{x^3}],$$

其中 $x=\overline{X}$，$y=\overline{Y}$，$y^2=x^3$. R 的分式域为

$$K=\boldsymbol{C}(V)=\boldsymbol{C}(x,y)=\boldsymbol{C}(x,x\sqrt{x})=\boldsymbol{C}(\sqrt{x}).$$

$\alpha=\sqrt{x}\in K$ 在 R 上是整的：$\alpha^2-x=0$，但 $\alpha\notin R$. 故 R 不是整闭的. 从另一方面看，K 是 $k=\boldsymbol{C}(x)$的二次扩张，k 是 $A=\boldsymbol{C}[x]$的分式域，A 在 K 的整闭包为 $B=\boldsymbol{C}[\sqrt{x}]\neq R$. B 是光滑曲线 $Y^2=X$ 的坐标环，是 Dedekind 环，K 也是 $Y^2=X$ 的函数域.

至于另一个例子 $O_K[X_1,\cdots,X_r]$，显然不是一维的，故不是 DD. 也不是 UFD，因 O_K 不是.

§2.6 理想的绝对范数

本节设 K 是 n 次数域，A 是其整数环.

定义 1 设 I 是 A 的整理想，则称 I 在 A 中的指数 $\# A/I$ 为 I 的绝对范(数)，记为 $N(I)$，这是一个正整数.

以下两个命题可说明这种定义的合理性.

命题 1 设非 0 整数 $\alpha\in A$，则 $N(A\alpha)=|N_{K/\boldsymbol{Q}}(\alpha)|$，后者定义见 §1.3.

证明 A 是秩为 n 的 Abel 群(或 $\boldsymbol{Z}$-模)，子模 $A\alpha$ 亦然(因为 $x\longmapsto x\alpha$ 给出模同构 $A\cong A\alpha$)，故存在 A 的一个 $\boldsymbol{Z}$-基 $e_1,\cdots,e_n$ 使 $A\alpha$ 有 $\boldsymbol{Z}$-基 $c_1e_1,\cdots,c_ne_n$ ($c_i\in\boldsymbol{Z}$)(事实上设 $\alpha_1,\cdots,\alpha_n$ 和

$\beta_1,\cdots,\beta_n$ 是 A 及 $A\alpha$ 的任意 $\mathbf{Z}$-基，则$(\beta_1,\cdots,\beta_n)=(\alpha_1,\cdots,\alpha_n)B$，$B$ 为 $\mathbf{Z}$ 上方阵，故存在 $\mathbf{Z}$ 上可逆方阵 P、Q 使 $PBQ=\mathrm{diag}(c_1,\cdots,c_n)$ 为对角形，于是令$(\alpha_1,\cdots,\alpha_n)P^{-1}=(e_1,\cdots,e_n)$，则$(\beta_1,\cdots,\beta_n)Q=(c_1e_1,\cdots,c_ne_n)$如上述．于是 $N(A\alpha)=\#(A/A\alpha)=c_1c_2\cdots c_n$．另一方面，$\alpha e_1,\cdots,\alpha e_n$ 显然也是 $A\alpha$ 的 $\mathbf{Z}$-基，于是有 A 的自同态：

$$A\xrightarrow{\sigma}A\alpha\xrightarrow{\tau}A\alpha,$$

$$e_i\longmapsto c_ie_i\longmapsto\alpha e_i,$$

记 $\varphi=\tau\sigma$：$e_i\longmapsto\alpha e_i$，则

$$N_{K/\mathbf{Q}}(\alpha)=\det(\varphi)=\det(\tau)\det(\sigma)=\pm\det(\sigma)$$

$$=\pm\det\begin{pmatrix}c_1&&\\&\ddots&\\&&c_n\end{pmatrix}=\pm c_1\cdots c_n.$$

这是由于 τ 是同构，从而 $\det\tau=\pm1$． □

命题 2 $N(IJ)=N(I)N(J)$对 A 的任意非零整理想 I 和 J 成立．

证明 由于 J 可分解，故只需证明 $N(I\wp)=N(I)N(\wp)$ 对任意非 0 理想 I 和素理想 $\wp$ 成立．由于 $N(I\wp)=\#A/I\wp=(\#A/I)(\#I/I\wp)=N(I)(\#I/I\wp)$，故只需证明

$$\#(A/\wp)=N(\wp)=\#(I/I\wp).$$

注意 $I/I\wp$ 是 A-模，且被 $\wp$ 零化，故是 $A/\wp$ 上线性空间，其子空间均为 A-子模，且应有形式 $Q/I\wp$（其中 Q 为理想且 $I\wp\subset Q\subset I$)．由于 $\wp$ 为素理想，故由理想的唯一分解性知 I 与 $I\wp$ 之间没有理想，故 $I/I\wp$ 在 $A/\wp$ 上是一维的，即得 $\#(I/I\wp)=\#(A/\wp)$． □

设 $k=\boldsymbol{F}_q(X)$是有限域 $\boldsymbol{F}_q$ 上的有理函数域，K 是 k 的有限扩张，A 是 $O_k=\boldsymbol{F}_q[X]$在 K 中的整闭包．对 A 的任一理想 I，$\# A/I$ 也是有限数，故也可定义 I 的绝对范 $N(I)$．这种代数函数域 K 与数域 K 的算术理论很相似．

第三章　素理想在扩域中的分解

§3.1　局部化

设 A 为整环，可能含许多（常为无限多）个素理想，为了便于解决问题，常设法把 A 化为另一环 A'，使 A' 只含较少的理想，甚至只有一个素理想．我们回忆由 $A=\mathbf{Z}$ 过渡到 $A'=\mathbf{Q}$ 时，非 0 素理想全都消去了．这是由于对每个素数 $p\in\mathbf{Z}$，$p\mathbf{Q}$ 含 $p\cdot\frac{1}{p}=1$，故 $p\mathbf{Q}=(1)$．由此可知"乘以分数"可以消去素理想．

定义 1　(i) 设 A 为整环，K 为其分式域，S 是 $A-\{0\}$ 中对乘法封闭的子集，且 $1\in S$，则环

$$S^{-1}A=\left\{\frac{a}{s}\,\middle|\,a\in A,s\in S\right\}\subset K$$

称为（A 对于 S 的）**分式环**(ring of fractions of A with respect to S)．

(ii) 记 $S_\wp=A-\wp$，其中 $\wp$ 为 A 的素理想，则环

$$S_\wp^{-1}A=\left\{\frac{a}{s}\,\middle|\,a,s\in A,s\notin\wp\right\}$$

称为（A 对于 $\wp$ 的）**局部化**(localization)．

显然 $A\subset S^{-1}A\subset K$，$\{1\}^{-1}A=A$，$\{A-\{0\}\}^{-1}A=K$.

例如 $A=\mathbf{Z}$ 时，$S=\{5^k\,|\,k=0,1,2,\cdots\}$对乘法封闭，则

$$\mathbf{Z}'=S^{-1}\mathbf{Z}=\left\{\frac{a}{5^k}\,\middle|\,k=0,1,\cdots,a\in\mathbf{Z}\right\}.$$

理想 $5\mathbf{Z}$ 在 $\mathbf{Z}'$ 中生成理想$(1)=\mathbf{Z}'$. $10\mathbf{Z}$ 生成 $10\mathbf{Z}'=2\mathbf{Z}'$.

再如令 $S_5=\mathbf{Z}-(5)$，则

$$S_5^{-1}\mathbf{Z}=\left\{\frac{a}{b}\,\middle|\,a,b\in\mathbf{Z},5\nmid b\right\}$$

易知当素理想 $p\mathbf{Z}\neq 5\mathbf{Z}$ 时(即 $p\neq 5$ 时)，总有 $p(S_5^{-1}\mathbf{Z})=(1)$.

一般地，A 的每个理想 I 生成

$A'=S^{-1}A$ 的一个理想

$$I'=IA'=S^{-1}I=\left\{\frac{a}{s}\,\middle|\,a\in I,s\in S\right\}$$

$$\begin{array}{ccc} A' & I'=(I'\cap A)A' \\ \varphi\downarrow & \uparrow\varphi^{-1} \\ A & I'\cap A \end{array}$$

事实上 IA' 的元素形如 $\sum_i a_i\frac{r_i}{s_i}(a_i\in I,r_i\in A,s_i\in S)$，即形如 $\sum_i\frac{a_i}{s_i}$(因为 $a_ir_i\in I$)，通分即知形如$\frac{a}{s}$. 当 I 与 S 相交时，则 $I'=(1)=A'$. 反之，A' 的每个理想 I' 也对应着 A 的理 想 $I'\cap A=I$.

定理 1 设 A 是整环，S 是 $A-\{0\}$的一个乘法封闭子集且 $1\in S$. 记 $A'=S^{-1}A$.

(1) A'的理想集到 A 的理想集有保序单射 φ: $I'\to I'\cap A$.

(2) A'的素理想半序集到 A 的与 S 不相交的素理想半序集有保序双射$\wp'\longmapsto\wp'\cap A$；其逆为$\wp\longmapsto\wp A'=S^{-1}\wp$.

证明 (1) 先证$(I'\cap A)A'=I'$. 显然$(I'\cap A)A'\subset I'A'=I'$. 另一方面，任取 $x=\frac{a}{s}\in I'$，则 $a=sx\in AI'\subset I'$，故 $x=\frac{a}{s}\in$

$(I'\cap A)A'$，即知$(I'\cap A)A'=I'$．故若$I'_1\cap A=I'_2\cap A$，则$I'_1=(I'_1\cap A)A'=(I'_2\cap A)A'=I'_2$，即知$\varphi$为单射．

(2) 若$\wp'$是A'的素理想，则$\wp=\wp'\cap A$是素理想（上章§2），且$\wp\cap S\subset\wp'\cap S=\varnothing$（因为$\wp'$是素理想）．反之设$\wp$是$A$的素理想，且与$S$不相交，要证$\wp'=\wp A'=S^{-1}\wp$为素理想．

事实上若$\frac{a_1}{s_1}\cdot\frac{a_2}{s_2}=\frac{p}{s_3}\in\wp'$，则$a_1a_2s_3=s_1s_2p\in\wp$．由于$s_3\notin\wp$，故$a_1a_2\in\wp$，故$a_1$或$a_2\in\wp$，即$a_1/s_1$或$a_2/s_2\in\wp'$，故$\wp'$是素理想（这里$a_i\in A, p\in\wp, s_i\in S$）．

由(1)可知，只需再证$(\wp A')\cap A=\wp$．显然左$\supset$右．任取A中元$x=\frac{p}{s}\in\wp A'$，则$sx=p\in\wp$，故$x\in\wp$，即知$(\wp A')\cap A=\wp$．　□

定理 2　设如定理 1.

(1) 若A是 Noether 环，则$S^{-1}A$是 Noether 环．

(2) 设B为A在R中的整闭包，则$S^{-1}B$是$S^{-1}A$在$S^{-1}R$中的整闭包，这里$R\supset A$为任一整环．

(3) 若A是整闭的，则$S^{-1}A$是整闭的．

(4) 若A是 Dedekind 环，则$S^{-1}A$是 Dedekind 环．

(5) 若$\wp$是 A 的极大理想，且与 S 不相交，则商环

$$A'/\wp'=(S^{-1}A)/\wp(S^{-1}A)=A/\wp.$$

(6) 设 A 是 Dedekind 环，$\wp$是其素理想，$S_\wp=A-\wp$，则A的局部化

$$A'=S_\wp^{-1}A=\left\{\frac{a}{b}\,\middle|\, b\notin\wp, a,b\in A\right\}$$

是主理想环，其唯一素理想$\wp'=\wp A'$是主理想$\pi A'=(\pi)$（其中$\pi\in A$），且A'的全部非 0 理想恰为

$$\wp'^n = (\pi^n), \qquad (n = 0,1,2,\cdots).$$

证明 (1) $S^{-1}A$ 的理想格到 A 的理想格有单射 φ(定理1),由极大条件即得.

(2) 任取$\frac{b}{s}\in S^{-1}B$ ($b\in B$, $s\in S$),由 b 在 A 上的整性方程

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1b - a_0 = 0 \quad (a_i \in A)$$

除以 s^n 即得$\frac{b}{s}$在 $S^{-1}A$ 上的整性方程

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s_n} = 0 \quad (a_i \in A).$$

故知 $S^{-1}B$ 在 $S^{-1}A$ 上整. 反之,若$\frac{r}{s}\in S^{-1}R$ 在 $S^{-1}A$ 上整,则由$\frac{r}{s}$的整性方程

$$\left(\frac{r}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}}\left(\frac{r}{s}\right)^{n-1} + \cdots + \frac{a_0}{s_0} = 0 \quad (a_i \in A,\ s_i \in S)$$

乘以$(s_0s_1\cdots s_{n-1})^n$ 即知 $rs_0\cdots s_{n-1}/s$ 在 A 上整,故

$$rs_0s_1\cdots s_{n-1}/s \in B$$

$$\frac{r}{s} \in (s_0\cdots s_{n-1})^{-1}B \subset S^{-1}B.$$

(3) 在(2)取 $R=K$ 为 A 的分式域即得.

(4) $S^{-1}A$ 为整闭 Noether 环,显然每个非 0 素理想均为极大理想.

(5) $A/\wp$ 显然可视为 $S^{-1}A/\wp(S^{-1}A)$的子环,这是因为 $\wp(S^{-1}A)\cap A=\wp$(定理 1(2)). 现任取 $x=\frac{a}{s}\in S^{-1}A$($a\in A$, $s\in S'\subset A$),则因 $s\not\equiv 0(\mathrm{mod}\ \wp)$(即 $s\notin\wp$)故知存在 $s'\in A$ 使

$$s's \equiv 1(\mathrm{mod}\ \wp)$$

故

$$as^{-1}-as'=as^{-1}(1-s's)\in \wp(S^{-1}A).$$

即知 $x(\mathrm{mod}\ \wp(S^{-1}A))=as'(\mathrm{mod}\ \wp)$，从而知

$$(S^{-1}A)/\wp(S^{-1}A)=A/\wp.$$

(6) 由定理 1(2)即知 $\wp'=\wp A'$ 是 A' 的唯一素理想．又因 A' 为 Dedekind 环，每一个理想必然是素理想之积，即为 $\wp'^n$ $(n=0,1,\cdots)$. 任取元素

$$\pi\in\wp-\wp^2$$

则 $(\pi)\subset\wp'$ 而 $(\pi)\not\subset\wp'^2$ 即 $\wp'\parallel(\pi)$，故 $(\pi)=\wp'$. 故 A' 的每个理想 $\wp'^n=(\pi)^n=(\pi^n)$ 均为主理想． □

有唯一极大理想的环称为**局部环**．上述定理 2(6)中 Dedekind 环 A 的局部化 A' 是局部环，而且还是主理想环．$\wp'$ 的生成元 π 称 A' 的**素元素**．易知 $\wp'-\wp'^2$ 中任一元可作素元. A' 中任一元 α 生成理想(α)，按定理 2(6)有

$$(\alpha)=\wp'^n=(\pi)^n=(\pi^n).$$

故 A' 的每个元素 α 均可表为

$$\alpha=u\pi^n,\qquad (u\ 为\ A_\wp\ 的单位，n\ 为非负整数).$$

K 中任意元显然可表为 $u\pi^n$，$n\in\mathbf{Z}$.

注记 1 定理 2(6)的逆(在一定意义上)也是对的：设 A 是一维 Noether 整环，若 A 对其每个非 0 素理想 $\wp$ 的局部化 $A_\wp$ 均为主理想环，则 A 必为 Dedekind 环．事实上，对于一维 Noether 整环 A 来说，以下三性质等价：(1)A 是整闭的；(2)A 的准素理想均为素理想的幂；(3)每个局部化 $A_\wp$ 均为主理想环. 而这第(3)条性质，即 $A_\wp$ 为主理想环(其中 $A_\wp$ 为一维 Noether 局部环)又等价于以下每一性质：(i)$A_\wp$ 是整闭的；(ii)

$A_\wp$是(某个)离散赋值(的赋值)环;(iii) $\wp' = \wp A_\wp$是主理想;(iv) $\wp'/\wp'^2$ 是 $A_\wp/\wp'$上一维线性空间;(V) $A_\wp$的非 0 理想均为$\wp'$的幂.

设 $A=C[V]$是平面曲线 V 的坐标环,A_P 是在点 P 的局部化(这里设 $P=(a_1,a_2)$, $\wp=(x-a_1,y-a_2)$, $A_P=A_\wp$). 于是 A_P 满足上述 5 个等价条件相当于 V 在 P 是光滑的. 因此$C[V]$(作为一维 Noether 环)是 Dedekind 环当且仅当 V 是光滑曲线(即在每一点都光滑).

习　题

1. 设 A 是主理想环而 K 是其分式域. 则 A 与 K 的中间环都是 A 的分式环(用 Bezout 等式).

2. 在定理 2(5)和(6)中,令 $A=\mathbf{Z}$, $\wp=(p)$. 重述定理并证明之.

3. 记号如定义 1. 设 $g: A\to B$ 是环同态且 $g(s)$是 B 的单位(对任一 $s\in S$),则存在唯一的环同态 $h: S^{-1}A\to B$ 使 $g=hf$,其中 f 是自然同态 $f: A\to S^{-1}A$, $x\longmapsto x/1$.

§3.2　素分解

本章总是设 L/K 为 n 次可分扩域,K 是 Dedekind 环 A 的分式域,A 在 L 中的整闭包为 B. 当 K 和 L 为数域时, $A=O_K$, $B=O_L$分别为 K 和 L 的整数环. 另一重要情形是代数函数域 L 和 K,即域 F 上有理函数域 $F(X)$的有限扩张. 以下总是设所有域扩张均是可分的.

定理 1　设 Dedekind 环 $A\subset B$ 如上,则 A 的每个素理想 $\wp$

(在 B 中生成的理想 $\wp B$)在 B 中分解为

$$(\wp)=\wp B=\mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\cdots\mathfrak{B}_g^{e_g}.$$

其中 $\mathfrak{B}_i$ 是 B 的互异素理想,e_i 为正整数($1\leqslant i\leqslant g$). 而且 $\{\mathfrak{B}_1,\cdots,\mathfrak{B}_g\}$ 恰为满足 $\mathfrak{B}\cap A=\wp$ 的 B 的素理想 $\mathfrak{B}$ 全体.

证明 由§2.3知 B 为 Dedekind 环,故其理想 $\wp B$ 应有如上形式的分解. 记 $\mathfrak{B}=\mathfrak{B}_i(1\leqslant i\leqslant g)$,则 $\mathfrak{B}\mid\wp B$,即 $\mathfrak{B}\supset\wp B$,故 $\mathfrak{B}\cap A\supset(\wp B)\cap A\supset\wp$,而 $\wp$ 为极大理想,故上式均为等号,即

$$\mathfrak{B}\cap A=(\wp B)\cap A=\wp.$$

反之,若 $\mathfrak{B}\cap A=\wp$ 对 B 的某素理想 $\mathfrak{B}$ 成立,则显然 $\mathfrak{B}\supset(\mathfrak{B}\cap A)B=\wp B$,即 $\mathfrak{B}\mid\wp B$. □

$A/\wp$ 可等同于 $B/\mathfrak{B}_i$ 的子环,二者均为域,分别记为 $\overline{A},\overline{B}$,或 $\overline{K},\overline{L_i}$. 因 B 是有限生成 A-模,故 $\overline{B}$ 是有限维 $\overline{A}$-空间,记扩域次数(维数)为

$$f_i=[\overline{B}:\overline{A}]=[\overline{L_i}:\overline{K}].$$

定义 1 记号如定理 1 中,

(1) e_i 称为 $\mathfrak{B}_i$ 对于 $\wp$ 的**分歧指数**(ramification index),f_i 称为 $\mathfrak{B}_i$ 对于 $\wp$ 的**剩余类次数**(residue class degree),g 称为 $\wp$ 在 B 中的不同素因子个数(有时也称为分裂指数),也记

$$e_i=e(\mathfrak{B}_i\mid\wp),\qquad f_i=f(\mathfrak{B}_i\mid\wp),\qquad g=g(\wp)=g_L(\wp).$$

(2) 若 $e_i>1$ 则称 $\mathfrak{B}_i$ 在 $\wp$ **上分歧**. 若存在 $e_i>1(1\leqslant i\leqslant g)$ 则称 $\wp$ 在 L **中分歧**. 若 $g=1,f_1=1,e_1=n$(即 $(\wp)=\mathfrak{B}_1^n$),则称 $\mathfrak{B}_1$ 在 $\wp$ **上完全分歧**;若 $g=n,f_i=1,e_i=1(1\leqslant i\leqslant g)$(即 $(\wp)=$

$\mathfrak{P}_1\cdots\mathfrak{P}_n$)则称$\wp$在$L$**完全分裂**.

(3) 定义$\mathfrak{P}$(=某$\mathfrak{P}_i$)的(从L到K的相对)**范**为

$$N_{L/K}(\mathfrak{P}) \doteq \wp^{f(\mathfrak{P}|\wp)}.$$

进而由积性定义L的任一分式理想$I=\prod\limits_{\mathfrak{P}}\mathfrak{P}^{v_{\mathfrak{P}}}$的范为$N_{L/K}(I)$ $=\prod\limits_{\mathfrak{P}}N_{L/K}(\mathfrak{P})^{v_{\mathfrak{P}}}$.

命题1 设$A\subset B\subset C$均为Dedekind环,分式域分别为$K\subset L\subset M$,均为可分扩张.B和C为A在L和M中的整闭包,设$\wp\subset\mathscr{Q}\subset\mathfrak{P}$分别为$A,B,C$中的非0素理想,$I$为$M$的理想,则

$$e(\mathfrak{P}|\wp)=e(\mathfrak{P}|\mathscr{Q})e(\mathscr{Q}|\wp),$$
$$f(\mathfrak{P}|\wp)=f(\mathfrak{P}|\mathscr{Q})f(\mathscr{Q}|\wp),$$
$$N_{M/K}(L)=N_{L/K}(N_{M/L}(I)).$$

证明 显然. □

定理2 记号如定理1,则

$$\sum_{i=1}^{g}e_if_i=[B/\wp B:A/\wp]=n.$$

证明 由于$(\wp B)\cap A=\wp$,故$B/\wp B$是$\overline{K}=A/\wp$上的向量空间.考虑序列

$$B\supset\mathfrak{P}_1\supset\mathfrak{P}_1^2\cdots\supset\mathfrak{P}_1^{e_1}\supset\mathfrak{P}_1^{e_1}\mathfrak{P}_2\supset\cdots\supset\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\supset\cdots\supset\wp B.$$

相邻两理想均形如$I\supset I\mathfrak{P}_i$,二者间无中间理想,故$I/I\mathfrak{P}_i$是$\overline{L}_i=B/\mathfrak{P}_i$上一维线性空间(参见上章末命题2证明),从而是$\overline{K}$上$f_i$维线性空间.对上述序列的每一项$I$均模以$\wp B$(与$I$的交),从

而成为 $\overline{K}$ 上线性空间的序列．相邻二空间的商空间同构于 $I/I\mathfrak{P}_i$，在 $\overline{K}$ 上是 f_i 维．故 $B/\wp B$ 在 $\overline{K}$ 上的维数 $[B/\wp B : A/\wp]$ 等于诸商空间维数之和，即为 $\sum_{i=1}^{g} e_i f_i$. 这就证明了第一等式.

对于第二个等式，当 A 是主理想环时是显然的，因为此时 B 作为 A—模有 A—基 $\alpha_1,\cdots,\alpha_n$，此即为 $B/\wp B$ 的 $A/\wp$—基（模以 $\wp B$）. 从而 $B/\wp B$ 在 $A/\wp$ 上维数为 n.

对一般情形，令 $S = A - \wp$，$A' = S^{-1}A = A_\wp$，$\wp' = \wp A'$，$B' = S^{-1}B$. 于是由 $\wp B = \prod \mathfrak{P}_i^{e_i}$ 可知

$$\wp' B' = \wp B' = \prod_{i=1}^{g} (B'\mathfrak{P}_i)^{e_i}.$$

$\mathfrak{P}_i' = B'\mathfrak{P}_i$ 是 B' 的非 0 素理想（由 $\mathfrak{P}_i \cap S = \wp \cap S = \varnothing$，及上节定理 1)，故由上述已证的第一个等式知

$$[B'/\wp' B' : A'/\wp'] = \sum_{i=1}^{g} e_i [B'/\mathfrak{P}_i' : A'/\wp']$$

$$= \sum_{i=1}^{g} e_i f_i,$$

后者是由于 $B'/\mathfrak{P}_i' \cong B/\mathfrak{P}_i$，$A'/\wp' \cong A/\wp$（上节定理 2(5)）. 再因 $A' = A_\wp$ 是主理想环，由上述已知 $[B'/\wp' B' : A'/\wp'] = n$（注意 $\wp A'$ 是 A' 的素理想，B' 是 A' 在 L 中的整闭包）. □

再考虑理想的范，对 A 的素理想 $\wp$，有

$$N_{L/K}(\wp B) = N_{L/K}(\prod_i \mathfrak{P}_i^{e_i}) = \prod_i (N_{L/K}\mathfrak{P}_i)^{e_i} = \prod_i \wp^{f_i e_i}.$$

故由定理 2 知 $N_{L/K}(\wp B) = \wp^n$. 由于 $N_{L/K}$ 是积性的，故知对 A 的任一理想 I，均有

$$N_{L/K}(I)=I^n.$$

命题 2 设 I 是 K 的理想,则

$$N_{K/Q}(I)=(N(I)).$$

也就是说,本节定义的理想的范与§2.6 定义的绝对范数是一致的.

证明 由于 $N_{K/Q}$ 与 N 均是积性的,只需对 $I=\wp$ 为素理想的情形证明. 设 $\wp\cap\mathbf{Z}=(p)$,则 $N_{K/Q}(\wp)=(p)^f$,其中 $f=f(\wp|p)=[A/\wp:\mathbf{Z}/(p)]$. 而 $N(\wp)=\#A/\wp=p^f$. □

在以后讨论 Galois 扩张 L/K 的素分解之后,我们还会看到,$N_{L/K}\mathfrak{P}=\prod_{\sigma\in G}\sigma\mathfrak{P}$(其中 $G=\mathrm{Gal}(L/K)$). 而且对任意(非 Galois)扩张 L/K,$\alpha\in L$,总有 $N_{L/K}(\alpha)=(N_{L/K}(\alpha))$,亦即 $N_{L/K}(\alpha B)=N_{L/K}(\alpha)B$,即理想的范与元素的范的定义是一致的.

§3.3 Kummer 定理

Kummer 定理明显给出素分解的一个常用方法.

设环 $A\subset B$ 如上节定理 1,$\wp\subset\mathfrak{P}$ 为 A 和 B 的非 0 素理想. 记 $\overline{A}=A/\wp$,$\overline{B}=B/\mathfrak{P}$. 对于任意

$$g(X)=b_nX^n+b_{n-1}X^{n-1}+\cdots+b_0\in A[X],$$

记
$$\overline{g}(X)=\overline{b}_nX^n+\overline{b}_{n-1}X^{n-1}+\cdots+\overline{b}_0\in\overline{A}[X].$$

称为 $g(X)$ 的模 $\wp$ 约化,其中 $\overline{b}_i=b_i+\wp$. 如果 $B=A[\alpha]$,即 B 的元素均为 α 的多项式(系数属于 A),我们要证明:$\wp B$ 的素分解与 α 的极小多项式 $f(X)$ 的约化 $\overline{f}(X)$ 的不可约分解相对应.

定理 1 (Kummer)　设 $B=A[\alpha]$为 Dedekind 环,如上节定理 1,$f(X)$为 α 满足的 $A[X]$中首一不可约多项式,$\wp$ 为 A 的非 0 素理想. 设 $f(X)$模 $\wp$ 约化 $\bar{f}(X)$在 $\bar{A}[X]$中有不可约因子分解

$$\bar{f}(X)=\bar{P}_1(X)^{e_1}\cdots\bar{P}_g(X)^{e_g},$$

其中 $P_i(X)\in A[X]$,$\bar{P}_i(X)$在 $\bar{A}[X]$中不可约且互异. 则

$$\wp B=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$$

为 $\wp B$ 的素分解,且 $f(\mathfrak{P}_i\ \ \wp)=\deg\bar{P}_i(X)$,其中素理想

$$\mathfrak{P}_i=(\wp,P_i(\alpha))=\wp B+P_i(\alpha)B.$$

$$\begin{array}{ccc}
B=A[\alpha] & \xrightarrow{\bmod \mathfrak{P}} & \bar{B}=\bar{A}[\bar{\alpha}] \\
| & & | \\
A & \xrightarrow{\bmod \wp} & \bar{A}
\end{array}$$

$$f(X)\longmapsto\bar{f}(X)=\bar{P}_1(X)^{e_1}\cdots\bar{P}_g(X)^{e_g}$$

$$\alpha\longmapsto\bar{\alpha}.$$

证明　1) 任给 $\mathfrak{P}\supset\wp$ 为 B 的素理想,记 $\bar{\alpha}$为 α 在模 $\mathfrak{P}$ 映射下的象. 由 $f(\alpha)=0$,知 $\bar{f}(\bar{\alpha})=0$,故 $\bar{\alpha}$是 $\bar{f}(X)$某一个不可约因子 $\bar{P}(X)$的根. 由此得到由 $\wp$ 的素理想因子集到 $\bar{f}(X)$的因子集的映射

$$\varphi:\ \mathfrak{P}\longmapsto\bar{P}(X).$$

反之,对 $\bar{f}(X)$的任一不可约因子 $\bar{P}_i(X)$,任取 $\bar{P}_i(X)$的一根 $\bar{\alpha}_i$

(属于 $\overline{A}$ 的某固定代数闭包)，则可定义映射

$$\mu: A[\alpha] \longrightarrow \overline{A}[\overline{\alpha}_i].$$

记
$$g(\alpha) \longmapsto \overline{g}(\overline{\alpha}_i).$$

$\mathfrak{P}_i=\ker\mu$ 是极大理想(因 $\overline{A}[\overline{\alpha}_i]\cong\overline{A}[X]/\overline{P}_i(X)$ 是域). 显然模 $\mathfrak{P}_i$ 映射(即 μ)映 α 为 $\overline{\alpha}_i$，故 $\varphi(\mathfrak{P}_i)=\overline{P}_i(X)$. 故知 φ 是 1∶1 对应.

2) 再证 $\mathfrak{P}_i=(\wp, P_i(\alpha))$. 由 $\mu(\wp)=0=\overline{P}_i(\overline{\alpha}_i)=\mu(P_i(\alpha))$ 知核 $\mathfrak{P}_i\supset(\wp, P_i(\alpha))$. 反之，设 B 中元 $g(\alpha)\in\mathfrak{P}_i$ ($g(X)\in A[X]$)，则模 $\mathfrak{P}_i$ 知

$$0=\overline{g}(\overline{\alpha})=\overline{g}(\overline{\alpha}_i) \qquad (\text{因 } \overline{\alpha}=\mu(\alpha)=\overline{\alpha}_i).$$

因 $\overline{P}_i(X)$ 是 $\overline{\alpha}_i$ 的极小多项式，故

$$\overline{g}(X)=\overline{P}_i(X)\overline{h}(X),$$
$$g(X)-P_i(X)h(X)\in\wp[X],$$
$$g(\alpha)-P_i(\alpha)h(\alpha)\in\wp[\alpha]\subset\wp B,$$
$$g(\alpha)\in\wp B+P_i(\alpha),$$

即知 $\mathfrak{P}_i\subset(\wp, P_i(\alpha))$，即 $\mathfrak{P}_i=(\wp, P_i(\alpha))$.

3) 最后证 $e_i=e'_i$, $\deg\overline{P}_i(X)=f'_i$, 这里 $e'_i=e(\mathfrak{P}_i\mid\wp)$, $f'_i=f(\mathfrak{P}_i\mid\wp)$. 后者显然：

$$\deg\overline{P}_i(X)=[\overline{A}[\overline{\alpha}_i]:\overline{A}]=[B/\mathfrak{P}_i:\overline{A}]=f(\mathfrak{P}_i\mid\wp).$$

又因

$$\begin{aligned}\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}&=(\wp, P_1(\alpha))^{e_1}\cdots(\wp, P_g(\alpha))^{e_g}\\&\subset(\wp, P_1(\alpha)^{e_1})\cdots(\wp, P_g(\alpha)^{e_g})\\&\subset(P_1(\alpha)^{e_1}\cdots P_g(\alpha)^{e_g}, \wp)\\&=(\wp)=\mathfrak{P}_1^{e'_1}\cdots\mathfrak{P}_g^{e'_g}.\end{aligned}$$

故知 $e_i\geqslant e'_i$(用到：$\overline{f}(X)=\prod\overline{P}_i(X)^{e_i}$, $f(X)-\prod P_i(X)^{e_i}\in\wp[X]$, $f(\alpha)-\prod P_i(\alpha)^{e_i}\in\wp[\alpha]$). 再由 $\sum e'f_i=n=\sum e_if_i$，即知 $e_i=e'_i$ $(1\leqslant i\leqslant g)$.

注记　若 $B=A[\alpha]$，则称 B 在 A 上有幂元整基(因为这时 $1,\alpha,\cdots,\alpha^{n-1}$ 是 B 的整基)，这并不总是可能的．但是，即使 $B\neq A[\alpha]$，只要

$$\wp\nmid\frac{\mathrm{Disc}(1,\alpha,\cdots,\alpha^{n-1})}{\mathrm{Disc}(L/K)},$$

则定理 1 仍然是成立的．这是由于此时由局部化可知有

$$B'=A'[\alpha],$$

其中 $A'=A_\wp=S^{-1}A,B'=S^{-1}B,S=A-\wp$．而由上节定理 2 的证明可知 $\wp B=\prod\mathfrak{P}_i^{e_i}$ 相当于 $\wp'B'=\prod\mathfrak{P}_i'^{e_i}(\wp'=\wp A')$.

习　题

1. 每个素数 $p\equiv1(\mathrm{mod}4)$ 均可表为平方和 $p=a^2+b^2(a,b\in\mathbf{Z})$.(提示：用 §2.5 习题 1 和素分解).

2. 可表为平方和的正整数集对乘法封闭．

3. 求自然数 n 可表为平方和的充分必要条件．

§3.4　分解群

本章以下部分讨论 Galois 扩域的素分解．

设 L/K 为 n 次 Galois 扩域，Galois 群 $\mathrm{Gal}(L/K)=G$，于是 G 中每个元素 σ 是 L 的一个 K-自同构(也是 L 到 K 的代数闭包 C 的 K-嵌入，不过 L 的嵌入象与自身相同：$\sigma L=L$).K 恰为在每个 $\sigma\in G$ 下都不动的 L 的元素全体．$\alpha\in L$ 的每个 K-共轭均在 L 中.L 恒可作为某个多项式的分裂域．

G 的每个子群 H，对应着其固定子域 $F(H)=\{\alpha\in L\mid\sigma\alpha=\alpha,\forall\sigma\in H\}$．而 $L\supset K$ 的每个中间域 F，对应着固定 F(中每个元

素)的子群 $H(F)\subset G$. 上述这种对应是 G 的子群集 $\{H\}$ 与 L/K 的中间域集 $\{F\}$ 间的 1∶1 对应,反序(对包含关系). F 为正规域(即 Galois 扩张)的充分必要条件为 $H(F)$ 是正规子群,此时 $\mathrm{Gal}(F/K)=G/H(F)$. 自然有 $H(F_1F_2)=H(F_1)\cap H(F_2)$.

以下总是设 L/K 为 n 次 Galois 扩张,K 是 Dedekind 环 A 的分式域,B 是 A 在 L 中的整闭包. 设所有的域扩张均是可分的. 设 $\wp$ 为 A 的素理想,在 B 中素分解为

$$\wp B=\mathfrak{B}_1^{e_1}\cdots\mathfrak{B}_g^{e_g}.$$

注意 B 对于 G 的作用封闭(若 $\alpha\in B,\sigma\in G$,由 $f(\alpha)=0$ 即可知 $(\sigma f)(\sigma\alpha)=0$,故 $\sigma\alpha\in B$,这里 $f\in A[X]$,是 α 满足的首一多项式,σf 是把 f 的系数以 σ 作用). 集合 $\{\mathfrak{B}_1,\cdots,\mathfrak{B}_g\}$ 在 G 作用下是封闭的;事实上对任意 $\mathfrak{B}_i$ 和 $\sigma\in G$,$\sigma\mathfrak{B}_i$ 也是素理想(由 $L/\sigma\mathfrak{B}_i=\sigma L/\sigma\mathfrak{B}_i=\sigma(L/\mathfrak{B}_i)$ 是域而知),且 $(\sigma\mathfrak{B}_i)\cap A=\sigma(\mathfrak{B}_i\cap A)=\sigma\wp=\wp$. 我们称 $\sigma\mathfrak{B}$ 与 $\mathfrak{B}$ 为**共轭理想**.

命题 1　G 在 $\{\mathfrak{B}_1,\cdots,\mathfrak{B}_g\}$ 上的作用是可迁的(即对任意 $\mathfrak{B}$, $Q\in\{\mathfrak{B}_1,\cdots,\mathfrak{B}_g\}$,存在 $\sigma\in G$ 使 $\mathfrak{B}=\sigma Q$; 也即 $\mathfrak{B}_1,\cdots,\mathfrak{B}_g$ 为相互共轭的理想).

证明　设 G 的元素为 $\sigma_1,\cdots,\sigma_n$ 且 $\sigma_1=1$. 若 $\mathfrak{B}\neq\sigma_1Q,\cdots,\sigma_nQ$,则由中国剩余定理(注意此时 $\mathfrak{B}$ 与诸 σ_iQ 均为极大理想,故是互素的),存在着 $x\in B$ 使

$$\begin{cases}x\equiv 0(\bmod\mathfrak{B}),\\ x\equiv 1(\bmod\sigma_1Q),\\ \cdots\cdots\\ x\equiv 1(\bmod\sigma_nQ).\end{cases}$$

故

$$N_{L/K}(x)=\sigma_1(x)\sigma_2(x)\cdots\sigma_n(x)\in\mathfrak{P}\cap A=\wp\subset Q.$$

(注意 $\sigma_1(x)=x\in\mathfrak{P}$,故 $N(x)\in\mathfrak{P}$),但由 $x\notin\sigma Q(\forall\ \sigma\in G)$ 知 $\sigma x\notin Q(\forall\ \sigma\in G)$,与上式矛盾. □

命题 2 对于 n 次 Galois 扩张 L/K,K 中素理想 $\wp$ 的分解必取形式:

$$\wp\ B=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e,$$

且 $e=e(\mathfrak{P}_1|\wp)=\cdots=e(\mathfrak{P}g|\wp)$,$f=f(\mathfrak{P}_1|\wp)=\cdots=f(\mathfrak{P}_g|\wp)$,进而有

$$efg=n.$$

证明 对于任意 i,j,由命题 1 知,存在 $\sigma\in G$ 使 $\mathfrak{P}_i=\sigma\mathfrak{P}_j$,于是由 $\wp\ B=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_i^{e_i}\cdots\mathfrak{P}_j^{e_j}\cdots\mathfrak{P}_g^{e_g}$,可知 $\wp\ B=\sigma(\wp\ B)=(\sigma\mathfrak{P}_1)^{e_1}\cdots(\sigma\mathfrak{P}_g)^{e_g}=(\sigma\mathfrak{P}_1)^{e_1}\cdots(\sigma\mathfrak{P}_i)^{e_i}\cdots(\mathfrak{P}_i)^{e_j}\cdots(\sigma\mathfrak{P}_g)^{e_g}$. 由因子分解唯一性即知 $e_j=e_i$. 同理知 $e_1=e_2=\cdots=e_g$. 再由 $f(\mathfrak{P}_i|\wp)=[B/\mathfrak{P}_i:A/\wp]=[B/\sigma\mathfrak{P}_j:A/\wp]=[\sigma(B/\mathfrak{P}_j):A/\wp]=[B/\mathfrak{P}_j:A/\wp]=f(\mathfrak{P}_j|\wp)$,即得命题. □

定义 1 设 L/K,$A\subset B$ 如上,$\wp$ 为 A 的素理想,$\mathfrak{P}$ 为 $\wp$ 在 B 中的素理想因子.

(i) 令

$$G_{\mathfrak{P}}=\{\sigma\in G\,|\,\sigma\mathfrak{P}=\mathfrak{P}\},$$

$G_{\mathfrak{P}}$ 称为 $\mathfrak{P}$ 的**分解群**(Decomposition Group),也记为 $D(\mathfrak{P}|\wp)$.

(ii) $G_{\mathfrak{P}}$(在 Galois 理论下)的固定子域 $L^d\subset L$ 称为 $\mathfrak{P}$ 的**分解域**.

记 $\mathfrak{P}=\mathfrak{P}_1$,若 $\sigma_2\mathfrak{P}=\mathfrak{P}_2(\sigma_2\in G)$,则显然陪集 $\sigma_2G_{\mathfrak{P}}$ 中元素均把 $\mathfrak{P}$ 变为 $\mathfrak{P}_2$,这也是能把 $\mathfrak{P}$ 变为 $\mathfrak{P}_2$ 的 G 中元全体(若 $\sigma\mathfrak{P}=\mathfrak{P}_2=\sigma_2\mathfrak{P}$,则 $\sigma_2^{-1}\sigma\mathfrak{P}=\mathfrak{P}$,故 $\sigma_2^{-1}\sigma\in G_{\mathfrak{P}}$,故 $\sigma\in\sigma_2G_{\mathfrak{P}}$). 因此,将 G 对

$G_{\mathfrak{P}}$ 作陪集分解

$$G=G_{\mathfrak{P}}\bigcup\sigma_2G_{\mathfrak{P}}\bigcup\cdots\bigcup\sigma_gG_{\mathfrak{P}},$$

则

$$\mathfrak{P}=\mathfrak{P}_1,\ \sigma_2\mathfrak{P}=\mathfrak{P}_2,\ \cdots,\ \sigma_g\mathfrak{P}=\mathfrak{P}_g.$$

恰为 $\wp$ 在 B 的素理想因子全体，特别可知

$$\#G_{\mathfrak{P}}=n/g=ef.$$

又 $\sigma\mathfrak{P}$ 的分解群显然为

$$G_{\sigma\mathfrak{P}}=\sigma G_{\mathfrak{P}}\sigma^{-1}.$$

(事实上，显然有 $(\sigma G_{\mathfrak{P}}\sigma^{-1})(\sigma\mathfrak{P})=(\sigma G_{\mathfrak{P}})\mathfrak{P}=\sigma\mathfrak{P}$；反之若 $\tau(\sigma\mathfrak{P})=\sigma\mathfrak{P}$ 则 $(\sigma^{-1}\tau\sigma)\mathfrak{P}=\mathfrak{P}$，则 $\sigma^{-1}\tau\sigma\in G_{\mathfrak{P}}$，故 $\tau\in\sigma G_{\mathfrak{P}}\sigma^{-1}$).

对分解群 $G_{\mathfrak{P}}$ 的兴趣来自于下列事实：$G_{\mathfrak{P}}$ 不改变 $\mathfrak{P}$，故可作用于 $\overline{B}=B/\mathfrak{P}$. $G_{\mathfrak{P}}$ 中的任一元 σ，把 $\mathfrak{P}$ 的一个陪集仍变为一个陪集，即对任一 $b\in B$，若记 $\overline{b}=b+\mathfrak{P}$，则

$$\sigma(\overline{b})=\sigma(b+\mathfrak{P})=\sigma b+\sigma\mathfrak{P}=\sigma b+\mathfrak{P}=\overline{\sigma b},$$

因此 σ 自然地可视为 $\overline{B}$ 在 $\overline{A}=A/\wp$ 上的自同构．即有群的自同态

$$\gamma:\ G_{\mathfrak{P}}\longrightarrow\overline{G}=\mathrm{Gal}(\overline{B}/\overline{A}),$$

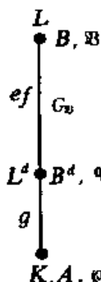
$$\sigma\longmapsto\overline{\sigma},\ \overline{\sigma}(\overline{b})=\overline{\sigma b}.$$

定理 1 设域 L/K 和环 $A\subset B$ 如上，$\mathfrak{P}$ 是 B 的素理想，$G_{\mathfrak{P}}$ 是 $\mathfrak{P}$ 的分解群，L^d 是其分解域，B^d 是 A 在 L^d 中的整闭包，$\mathfrak{q}=\mathfrak{P}\bigcap L^d=\mathfrak{P}\bigcap B^d$，$\wp=\mathfrak{P}\bigcap A$.

(1) $g_L(\mathfrak{q})=1$，即 $\mathfrak{q}$ 在 L 只一个素因子 $\mathfrak{P}$. 而且 L^d 是有此性质的最小中间域．

(2) $f(\mathfrak{q}|\wp)=e(\mathfrak{q}|\wp)=1$，$B^d/\mathfrak{q}=A/\wp$．

(3)$\overline{B}=B/\mathfrak{P}$ 是 $\overline{A}=A/\wp$ 的 Galois 扩张，且有群的满同态



$$\gamma:\ G_{\mathfrak{B}} \longrightarrow \overline{G} = \mathrm{Gal}(\overline{B}/\overline{A}),$$

$$\sigma \longmapsto \bar{\sigma},\ \bar{\sigma}(\bar{b}) = \overline{\sigma b}.$$

证 (1) 对任一中间域 E，记 $\mathfrak{q} = \mathfrak{B} \cap E$. 因 $\mathfrak{q}$ 在 L 的素理想因子均与 $\mathfrak{B}$ 共轭，故因子个数为 $g_L(\mathfrak{q}) = 1$ 相当于 $G(L/E)\mathfrak{B} = \mathfrak{B}$，这又相当于 $G(L/E) \subset G_{\mathfrak{B}}, E \supset L^d$.

(2) 由(1)知 $e(\mathfrak{B}/\mathfrak{q})f(\mathfrak{B}/\mathfrak{q}) = [L:L^d] = ef$，即 $e(\mathfrak{B}|\mathfrak{q}) = e, f(\mathfrak{B}/\mathfrak{q}) = f$，故知 $e(\mathfrak{q}|\wp) = f(\mathfrak{q}|\wp) = 1$. 后者说明 $B^d/\mathfrak{q} = A/\wp$.

(3) 任取 $\bar{x} \in \overline{B}$，x 在 A 上满足一首一不可约多项式 $f(X)$，其根 $x_i \in B$(因 L 是 Galois 扩张)，故(系数模 $\wp$ 后)$\bar{f}(X)$的根 $\bar{x}_i$ 均属于 $\overline{B}$，即知 $\overline{B}/\overline{A}$ 是正规扩张，即 Galois 扩张.

再证自然同态 $G_{\mathfrak{B}} \longrightarrow \overline{G}$ 是满射. 可设有限扩张 $\overline{B}/\overline{A}$ 由 $\bar{\alpha}$ 生成，即 $\overline{B} = \overline{A}[\bar{\alpha}], \alpha \in B$. 设 α 在 B^d 上的首一最小多项式为 $f(X)$. 于是 $\bar{\alpha}$ 在 $\overline{A}$ 上的极小多项式是 $\bar{f}(X)$的因子. $\overline{G}$ 中的每个元素 σ' 由 $\sigma'\bar{\alpha}$ 决定，$\sigma'\bar{\alpha}$ 是 $\bar{f}(X)$的根. 由于 $G_{\mathfrak{B}}$ 可迁地作用于 $f(X)$的根，故必存在 $\sigma \in G_{\mathfrak{B}}$ 使 $\overline{\sigma\alpha} = \sigma'\bar{\alpha}$，即 $\bar{\sigma} = \sigma'$. □

§3.5 惯性群

继续上节讨论，$G_{\mathfrak{B}}$ 为 $\mathfrak{B}$ 的分解群，自然映射

$$\gamma:\ G_{\mathfrak{B}} \longrightarrow \overline{G},\ \sigma \longmapsto \bar{\sigma}.$$

定义 1 $T_{\mathfrak{B}} = \mathrm{Ker}(\gamma)$ 称为 $\mathfrak{B}$ 的**惯性群**(Inertia Group, Trägheitsgruppe)，也记为 $T(\mathfrak{B}|\wp)$. 其固定子域记为 L^i，称为 $\mathfrak{B}$ 的**惯性域**.

显然有

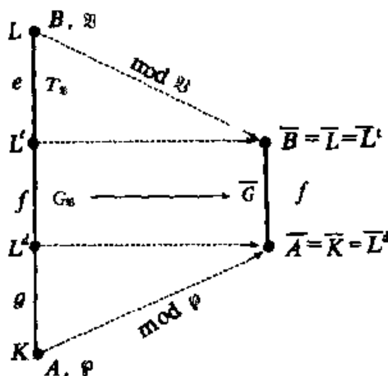
$$\begin{aligned}T_{\mathfrak{P}} &= \{\sigma\in G_{\mathfrak{P}} \mid \bar{\sigma}=1\}\\ &= \{\sigma\in G_{\mathfrak{P}} \mid \bar{\sigma}(\bar{\alpha})=\bar{\alpha}\ \text{对任意}\ \bar{\alpha}\in\bar{B}\}\\ &= \{\sigma\in G_{\mathfrak{P}} \mid \sigma(\alpha)\equiv\alpha \bmod \mathfrak{P}\quad \text{对任意}\ \alpha\in B\}\\ &= \{\sigma\in G \mid \sigma(\alpha)\equiv\alpha \bmod \mathfrak{P}\quad \text{对任意}\ \alpha\in B\}.\end{aligned}$$

最后的等号是由于,取 $\alpha\in\mathfrak{P}$ 则 $\sigma(\alpha)\equiv\alpha\in\mathfrak{P}$,故知 $\sigma\in G_{\mathfrak{P}}$.

由定义知 $T_{\mathfrak{P}}$ 是 $G_{\mathfrak{P}}$ 的正规子群,故 $L/L^t, L^t/L^d$ 均为Galois扩张,且 $\mathrm{Gal}(L/L^t)=T_{\mathfrak{P}}$, $\mathrm{Gal}(L^t/L^d)=G_{\mathfrak{P}}/T_{\mathfrak{P}}\cong\bar{G}$. 特别可知 $[L^t:L^d]=\#\bar{G}=f$. 从而 $e=[L:L^t]$, $g=[L^d:K]$. 记 $\mathfrak{P}^t=\mathfrak{P}\cap L^t$, $B^t=B\cap L^t$.

命题 1 $e(\mathfrak{P}|\mathfrak{P}')=e,\qquad f(\mathfrak{P}|\mathfrak{P}')=1,$

$e(\mathfrak{P}'|\mathfrak{q})=1,\qquad f(\mathfrak{P}|\mathfrak{q})=f.$



证 先证 $f(\mathfrak{P}|\mathfrak{P}')=1$. 任取 $\theta\in\bar{B}$,取 $\alpha\in B$ 使 $\bar{\alpha}=\theta$. 则

$$g(X)=\prod_{\sigma\in T_{\mathfrak{P}}}(X-\sigma\alpha)\in B^t[X].$$

系数模 $\mathfrak{P}$ 之后 $\bar{g}(X)\in\bar{B}^t[X]$. 但 $\overline{\sigma\alpha}=\bar{\sigma}\bar{\alpha}=1\cdot\theta=\theta$ (对所有 $\sigma\in T_{\mathfrak{P}}$),故 $\bar{g}(X)=(X-\theta)^m$, $m=\#T_{\mathfrak{P}}$. 而 $\mathrm{Gal}(\bar{B}/\bar{B}^t)$中每个同

构 $\bar{\sigma}$ 映 θ 为 $\bar{g}(X)$另一根，仍为 θ. 故 $\mathrm{Gal}(\bar{B}/\bar{B'})=1$, $\bar{B}=\bar{B'}$, $f(\mathfrak{B}|\mathfrak{B}')=1$. 再由 $f(\mathfrak{q}|\wp)=1$ 知 $f(\mathfrak{B}'|\mathfrak{q})=f$. 于是知 $e(\mathfrak{B}'|\mathfrak{q})=1$. 由上节 $e(\mathfrak{B}|\wp)=1$ 知 $e(\mathfrak{B}|\mathfrak{B}')=e$. □

也就是说，对于 $\mathfrak{B}$ 下的素理想有：L/L^t 是完全分歧的，L^t/K 是非分歧的，L^d/K 是(至少 2)分裂的，L/L^d 是不分裂的(即 $\mathfrak{q}$ 上只一个因子).

现设 K' 是 L/K 的中间域，令 $\wp'=\mathfrak{B}\cap K'$，A' 为 A 在 K' 的整闭包，G' 是 K' 的固定子群．令 $G'_{\mathfrak{B}}=D(\mathfrak{B}|\wp')$，$T'_{\mathfrak{B}}=T(\mathfrak{B}|\wp')$ 为 $\mathfrak{B}$ 在 $\wp'$ 的分解群和惯性群．由定义易知有

$$G'_{\mathfrak{B}}=G_{\mathfrak{B}}\cap G',\qquad T'_{\mathfrak{B}}=T_{\mathfrak{B}}\cap G'.$$

故

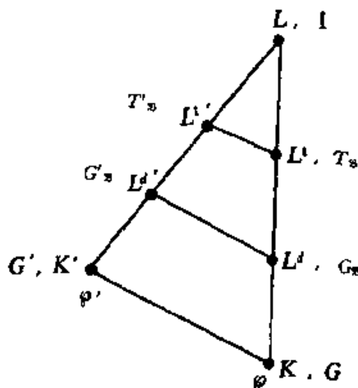
$$L^{d'}=L^dK',\qquad L^{t'}=L^tK'.$$

其中 $L^{d'}$，$L^{t'}$ 为 $\mathfrak{B}$ 对于 $\wp'$ 的分解域和惯性域．故有

命题 2 (1) $L^d\subset K'$ 当且仅当 $\wp'B$ 是 $\mathfrak{B}$ 的幂．

(2) $L^d\supset K'$ 当且仅当 $e(\wp'|\wp)=f(\wp'|\wp)=1$.

(3) $L^t\subset K'$ 当且仅当 $\mathfrak{B}$ 对 $\wp'$ 完全分歧．



(4) $L^t\supset K'$当且仅当$e(\wp'\mid\wp)=1$.

(5) 若$\wp$在L_1,L_2均非分歧,则在L_1L_2非分歧.

(6) 若$\wp$在L_1,L_2均完全分裂,则在L_1L_2完全分裂.

证 (1) $\wp'B$是$\mathfrak{B}$的幂$\Leftrightarrow K'=L^d=L^dK'\Leftrightarrow L^d\subset K'$.

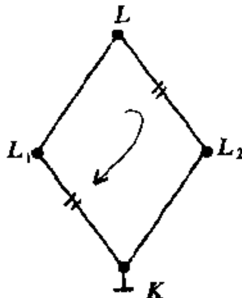
(2) $e(\wp'\mid\wp)=f(\wp'\mid\wp)=1\Leftrightarrow e(\mathfrak{B}\mid\wp')f(\mathfrak{B}\mid\wp')=ef$ $\Leftrightarrow L^d=L^{d'}=L^dK'\Leftrightarrow K'\subset L^d$.

(3) 和(4)可与(1),(2)类似证明.(5)记$L=L_1L_2$,由(4)知$L_1,L_2\subset L^t$,故$L\subset L^t$,即$L=L^t$.(6)同样可证. □

设$\mathfrak{B}_i=\sigma_i\mathfrak{B}$,$\sigma_i\in G$. 则显然$\mathfrak{B}_i$的分解域为$\sigma_iL^d$,惯性域为$\sigma_iL^t$. 注意$L^d$不一定是正规域($G_{\mathfrak{B}}$不一定是$G$的正规子群),故可能$L^d\neq\sigma_iL^d$. 因此$\mathfrak{q}_i=\mathfrak{B}_i\cap\sigma_iL^d=\sigma_i\mathfrak{q}$在$L^d$的分解情形并不清楚(只能知道$\wp$在$L^d$中分解为$(\wp)=\mathfrak{q}M$,$M$与$\mathfrak{q}$互素). 但若$G_{\mathfrak{B}}$为正规子群,$L^d/K$为Galois扩张,则$L^d=\sigma_iL^d$同为任一$\mathfrak{B}_i$的分解域,故$\wp$在$L^d$完全分解:$(\wp)=\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_g$. 再若$T_{\mathfrak{B}}$为$G$的正规子群,则$L^t=\sigma_iL^t$同时为所有$\mathfrak{B}_i$的惯性域,故每个$\mathfrak{q}_i$在$L^t$均仍为素理想,每个$\mathfrak{q}_i$到$L$后均分解为素理想$\mathfrak{B}_i$的$e$次幂$(\mathfrak{q}_i)=\mathfrak{B}_i^e$.

设$L=L_1L_2$, L_1/K为Galois扩张,$\mathrm{Gal}(L_1/K)=G_1$,则易知L/L_2为Galois扩张,且$\mathrm{Gal}(L/L_2)$可视为G_1的子群. 事实上,任一$\sigma\in\mathrm{Gal}(L/L_2)$限制到$L_1$上后可视为$G_1$中元素,故有群的(限制)同态:

$$S:\quad \mathrm{Gal}(L/L_2)\longmapsto G_1$$



且显然是单射.($S(\sigma)=1$意味着σ保持L_1的元素不动,而σ又保持L_2中元素不动(因属于$\mathrm{Gal}(L/L_2)$,故保持L的元素不动),故S为群的嵌入.

现设 $\mathfrak{P}$ 为 L 的素理想，$\wp=\mathfrak{P}\cap A$，$\mathfrak{q}_i=\mathfrak{P}\cap B_i$（$B_i$ 是 A 在 L_i 中整闭包，对于数域的情形，$B_i=O_{L_i}$）。

命题 3 （1）分解群 $D(\mathfrak{P}|\mathfrak{q}_2)$ 可视为 $D(\mathfrak{q}_1|\wp)$ 的子群．

（2）惯性群 $T(\mathfrak{P}|\mathfrak{q}_2)$ 可视为 $T(\mathfrak{q}_1|\wp)$ 的子群．

证明 （1）$\sigma\in D(\mathfrak{P}|\mathfrak{q}_2)$ 意味着 $\sigma\in \mathrm{Gal}(L/L_2)$ 且 $\sigma\mathfrak{P}=\mathfrak{P}$．从而 σ 可视为 G_1 中元素且 $\sigma\mathfrak{q}_1=\sigma(\mathfrak{P}\cap B_1)=(\sigma\mathfrak{P})\cap(\sigma B_1)=\mathfrak{P}\cap B_1=\mathfrak{q}_1$，即知 $\sigma\in D(\mathfrak{q}_1|\wp)$．

（2）$\sigma\in T(\mathfrak{P}|\mathfrak{q}_2)$ 意味着 $\sigma\in \mathrm{Gal}(L/L_2)$，且对 $\alpha\in B$ 有 $\sigma\alpha\equiv\alpha(\mathrm{mod}\,\mathfrak{P})$．故 $\sigma\in G_1$ 且对 $\alpha\in B_1$ 有 $\alpha\equiv\alpha(\mathrm{mod}\,\mathfrak{q}_1)$（因为 $\mathfrak{q}_1=\mathfrak{P}\cap B_1$）．即知 $\sigma\in T(\mathfrak{q}_1|\wp)$． □

习　题

1．设如命题 3．证明"非分歧性"和"全分裂性"均可提升，即若 $\mathfrak{q}_1|\wp$ 非分歧，则 $\mathfrak{P}|\mathfrak{q}_2$ 非分歧；若 $\mathfrak{q}_1|\wp$ 完全分裂，则 $\mathfrak{P}|\mathfrak{q}_2$ 完全分裂．

2．设如命题 1，而 L/K 为 Abel 扩张，证明 $G_{\mathfrak{P}}$ 和 $T_{\mathfrak{P}}$ 均只依赖于 $\wp$．

§3.6　Frobenius 自同构与 Artin 映射

现在继续上节讨论，但进一步设剩余类域是有限的，即设

$$N\wp=\#A/\wp=\#\overline{K}=q$$

为有限的，这里 $\wp$ 为 K 的素理想，K 是 A 的分式域，L/K 为 n 次 Galois 扩张，$\mathfrak{P}$ 为 $\wp$ 在 L 的素理想因子．（例如当 K 为数域时，设 $\wp\cap\mathbf{Z}=(p)$，则 $\overline{K}$ 是 $\overline{\boldsymbol{Q}}=\mathbf{Z}/p\mathbf{Z}=\boldsymbol{F}_p$ 的 $f(\wp|p)$ 次扩张，q

$=p^{f(\wp|p)}$是有限的．当 K 为有限域上一元函数域时，q 也有限）．于是 $\overline{L}=B/\mathfrak{P}$ 是 $\overline{K}$ 的 $f=f(\mathfrak{P}|\wp)$次扩张（这里 B 是 A 在 L 的整闭包）．由有限域知识可知，$\boldsymbol{F}_{q^f}/\boldsymbol{F}_q$ 的 Galois 群是循环群，生成元为 Frobenius 自同构 $\varphi: \alpha \longmapsto \alpha^q$．因此可知 $\overline{G}=\mathrm{Gal}(\overline{L}/\overline{K})$是 f 阶循环群，设 $\overline{G}$ 的生成元为 $\bar{\sigma}$，$\bar{\sigma}$ 是 $\sigma\in G_{\mathfrak{P}}$ 在同构 $G_{\mathfrak{P}}/T_{\mathfrak{P}}\cong\overline{G}$ 下的象，$\bar{\sigma}$ 由下式刻画：

$$\bar{\sigma}(\bar{\alpha})=\bar{\alpha}^{N\wp} \qquad (\forall\ \bar{\alpha}\in\overline{L}) \qquad (*)$$

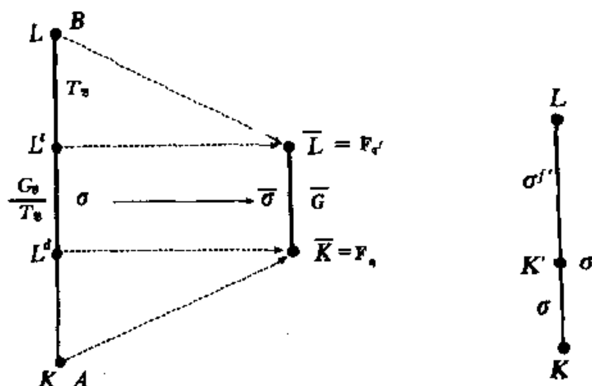
$\bar{\sigma}$ 在 $G_{\mathfrak{P}}$ 的原象是一个陪集 $\sigma T_{\mathfrak{P}}$，记为$(\mathfrak{P},L/K)$．显然，$\sigma T_{\mathfrak{P}}$ 只有一个元素$\Leftrightarrow T_{\mathfrak{P}}=1\Leftrightarrow\mathfrak{P}$ 对 K 非分歧；此时记 $\bar{\sigma}$ 的唯一原象

$$\sigma=(\mathfrak{P},\ L/K) \qquad \text{或} \qquad \left(\frac{L/K}{\mathfrak{P}}\right),$$

称为 $\mathfrak{P}$ 对 K 的 **Frobenius 自同构（符号）**．由（$*$）可知，对任一 $\sigma\in G_{\mathfrak{P}}$，$\sigma=(\mathfrak{P},L/K)$当且仅当

$$\sigma\alpha\equiv\alpha^{N\wp} \qquad (\mathrm{mod}\quad \mathfrak{P}). \qquad (\forall\ \alpha\in\mathfrak{P})$$

进一步，对 $\sigma\in\mathfrak{G}$，只要 σ 满足上式，也有 $\sigma=(\mathfrak{P},L/K)$．（因为由上式即可知 $\sigma\mathfrak{P}\subset\mathfrak{P}$，即 $\sigma\in G_{\mathfrak{P}}$）．



命题 1　设 L/K 为 Galois 扩张，K 的素理想 $\wp$ 在 L 的素理想因子 $\mathfrak{B}$ 对 K 非分歧，K 的剩余类域 $\bar{K}$ 是 $q=N\wp$ 元有限域．则

(i) Frobenius　自同构 $(\mathfrak{B},L/K)$ 是 $f(\mathfrak{B}\mid\wp)$ 阶循环群 $G_{\mathfrak{B}}$（即 $\mathfrak{B}$ 的分解群）的生成元．且对 $\sigma\in G$，$\sigma=(\mathfrak{B},L/K)$ 当且仅当

$$\sigma\alpha\equiv\alpha^{N\wp}\ (\mathrm{mod}\,\mathfrak{B})\qquad(\forall\ \alpha\in B).$$

(ii) 对任意 $\tau\in G$，$\tau\mathfrak{B}$ 的 Frobenius 自同构为

$$(\tau\mathfrak{B},L/K)=\tau(\mathfrak{B},L/K)\tau^{-1}.$$

(iii) 设 K' 为 L/K 的中间域，$\wp'=\mathfrak{B}\cap K'$，则

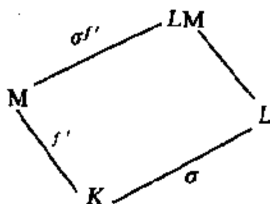
$$(\mathfrak{B},L/K')=(\mathfrak{B},L/K)^{f(\wp'|\wp)}.$$

(iv) 若(iii)中 K'/K 为 Galois 扩张，则

$$(\mathfrak{B},L/K)|_{K'}=(\wp',K'/K).$$

(v)设 M 为 K 的任一有限扩张，$\mathfrak{B}'$ 是 $\mathfrak{B}$ 在 LM 中任一素理想因子，$\wp'=\mathfrak{B}'\cap M$. 则 $\mathfrak{B}'$ 对 M 非分歧且

$$(\mathfrak{B}',LM/M)|_L=(\mathfrak{B},L/K)^{f(\wp'|\wp)}.$$



证明　(i) 已证过．

(ii) 显然 $\tau\mathfrak{B}$ 也非分歧，而由 $(\mathfrak{B},L/K)(\tau^{-1}\alpha)\equiv(\tau^{-1}\alpha)^q$ $(\mathrm{mod}\ \ \mathfrak{B})(\forall\ \alpha\in B)$，
可知

$$(\tau(\mathfrak{B},L/K)\tau^{-1})\alpha\equiv\alpha^q\quad(\mathrm{mod}\quad\tau\mathfrak{B})(\forall\ \alpha\in B).$$

(iii) $(\mathfrak{B},L/K)^{f(\wp'|\wp)}(\alpha)\equiv\alpha^{qf(\wp'|\wp)}\equiv\alpha^{N\wp'}(\mathrm{mod}\mathfrak{B})(\forall\ \alpha\in B)$.

(iv)由

$$(\mathfrak{B},L/K)\alpha\equiv\alpha^q(\mathrm{mod}\mathfrak{B})(\forall\ \alpha\in B),$$

知　　$(\mathfrak{B},L/K)\alpha\equiv\alpha^q(\mathrm{mod}\mathfrak{B}\cap K')(\forall\ \alpha\in B\cap K')$.

(v)由上节命题 1 知 $\mathfrak{P}'$对 M 的惯性群是 $\mathfrak{P}$ 对 K 的惯性群(=1)的子群,故 $\mathfrak{P}'$对 M 非分歧,而

$$(\mathfrak{P}', LM/M)\alpha \equiv \alpha^{N\wp'} \equiv \alpha^{q^{f(\wp'|\wp)}}$$
$$\equiv (\mathfrak{P}, L/K)^{f(\wp'|\wp)}(\alpha) \pmod{\mathfrak{P}} \ (\forall\ \alpha \in B). \square$$

现在设 L/K 为 Abel 扩张,设 K 的素理想$\wp$在 L 非分歧.于是由命题 1(ii)可知,$\wp$ 在 L 的所有素理想因子 $\mathfrak{P}$(或 $\tau\mathfrak{P}$)的 Frobenius 自同构是相同的,记为

$$(\wp, L/K) = (\mathfrak{P}, L/K),$$

也称为$\wp$的 **Artin 自同构(符号)**.

Artin(Frobenius)符号的深层意义在于:它把 K 的一个素理想$\wp$对应到 K 的扩张 L/K 的 Galois 群 $G(L/K)$中一个元素 $(\wp, L/K)$:

$$\wp \longmapsto (\wp, L/K).$$

我们可以把此映射积性地拓广到 K 的一般分式理想上去,只要这个理想不含分歧的素理想因子.详言之,记$\boldsymbol{I}(d)$为与 K 的判别式 d 互素的 K 的分式理想子群,对于$\boldsymbol{I}(d)$中任一理想 $I=\prod \wp^{v_\wp}$,定义 I 的 **Artin 符号**为

$$(I, L/K) = \prod(\wp, L/K)^{v_\wp}.$$

于是,Artin 符号就建立了理想群到 Galois 群的同态映射

$$\omega: \boldsymbol{I}(d) \longrightarrow G(L/K),$$
$$I \longmapsto (I, L/K),$$

ω 称为 **Artin(互反律)映射**.可以证明,ω 是满射,它的核"基本上"就是范,即 $\mathscr{N}(d) = \{N_{L/K}\mathfrak{P} \mid \mathfrak{P}$ 为 L 的与 d 互素的理想$\}$.(事实上,Ker $\omega = \mathscr{P}_d\mathscr{N}(d)$,其中 $\mathscr{P}_d$ 是某些主理想集).因此有类群到 Galois 群的同构:

$$\boldsymbol{I}(d)/\mathrm{Ker}\omega \cong G(L/K).$$

这就引向著名的"类域论".

§3.7. 二次域等域中的素分解

设 $K=\boldsymbol{Q}(\sqrt{d})$ 为二次数域, d 为无平方因子有理整数. 此时总有

$$O_K=\boldsymbol{Z}[\alpha],$$

$$\alpha=\begin{cases}\sqrt{d}, & \text{当 } d\equiv 2 \text{ 或 } 3 \pmod 4,\\ \dfrac{1+\sqrt{d}}{2}, & \text{当 } d\equiv 1 \pmod 4.\end{cases}$$

我们用 Kummer 定理来研究素 p 在 K 中的分解.

1. 先设 $d\equiv 2$ 或 $3 \pmod 4$, 于是 $\alpha=\sqrt{d}$, 它在 $\boldsymbol{Q}$ 上的最小多项式为

$$f(X)=X^2-d.$$

模以 p, 在 $\boldsymbol{F}_p=\boldsymbol{Z}/p\boldsymbol{Z}$ 上分解情形有三种:

$$\bar{f}(X)=X^2-\bar{d}=\begin{cases}X^2, & \text{当 } \bar{d}=0\in\boldsymbol{F}_p,\\ (X-\bar{a})(X+\bar{a}), & \text{当 } \bar{d}\in\boldsymbol{F}_p^{*2},\\ X^2-\bar{d}, & \text{否}.\end{cases}$$

情形 2 相当于 d 是模 p 的平方剩余, 即 $\left(\frac{d}{p}\right)=1$, 且设 $d\equiv a^2 \pmod p$; 情形 3 相当于 d 是模 p 的非平方剩余, 即 $\left(\frac{d}{p}\right)=-1$. 由 Kummer 定理可知相应有三种分解情形:

$$pO_K=\begin{cases}\wp^2, & \wp=(p,\sqrt{d}),\\ \wp_1\wp_2, & \wp_1=(p,\sqrt{d}-a),\ \wp_2=(p,\sqrt{d}+a),\\ \wp, & \wp=(p,d-d)=(p).\end{cases}$$

注意在情形 2，当 $p\neq 2$ 时，$\wp_1\neq\wp_2$，因为$(x-\bar{a})$和$(x+\bar{a})$是不同因子.

2. 再设 $d\equiv 1 \pmod 4$，则 $\alpha=\dfrac{1+\sqrt{d}}{2}$的极小多项式为

$$f(X)=\left(X-\frac{1+\sqrt{d}}{2}\right)\left(X-\frac{1-\sqrt{d}}{2}\right)=X^2-X+\frac{1-d}{4}.$$

(i) 当 $p\neq 2$ 时，

$$f(X)=\left(X-\frac{1}{2}\right)^2-\frac{d}{4},$$

故在 $\boldsymbol{F}_p$ 上有分解：

$$\bar{f}(X)=\begin{cases}\left(X-\left(\overline{\dfrac{1}{2}}\right)\right)^2, & \text{当 } p\mid d,\\ \left(X-\left(\overline{\dfrac{1+a}{2}}\right)\right)\left(X-\left(\overline{\dfrac{1-a}{2}}\right)\right), & \text{当 } d\equiv a^2 \pmod p,\\ X^2-X+\left(\overline{\dfrac{1-d}{4}}\right), & \text{当 } d\not\equiv a^2 \pmod p\ (\forall\ a).\end{cases}$$

由 Kummer 定理可知相应有分解

$$pO_K=\begin{cases}\wp^2, & \wp=\left(p,\dfrac{1+\sqrt{d}}{2}-\dfrac{1}{2}\right)=(p,\sqrt{d}),\\ \wp_1\wp_2, & \wp_i=\left(p,\dfrac{1+\sqrt{d}}{2}-\dfrac{1\pm a}{2}\right)=(p,\sqrt{d}\mp a),\\ \wp, & \wp=(p).\end{cases}$$

注意$(p,\sqrt{d}/2)=(p,\sqrt{d})$，$\left(p,\dfrac{\sqrt{d}\mp a)}{2}\right.=(p,\sqrt{d}\mp a)$(由于 2 与 p 互素).

(ii) 当 $p=2$ 时，模 2 有

$$\frac{1-d}{4}\equiv\begin{cases}0, & \text{当 } d\equiv 1(\text{mod}8),\\ 1, & \text{当 } d\equiv 5(\text{mod}8).\end{cases}$$

故

$$\bar{f}(X)=\begin{cases}X^2-X=X(X+\bar{1}), & \text{当 } d\equiv 1(\text{mod } 8),\\ X^2+X+1\quad, & \text{当 } d\equiv 5(\text{mod } 8).\end{cases}$$

相应有分解

$$2O_K=\begin{cases}\wp_1\wp_2, & \wp_1=(2,\frac{1+\sqrt{d}}{2}),\wp_2=(2,\frac{1+\sqrt{d}}{2}-1),\\ \wp, & \wp=(2).\end{cases}$$

总之，我们有如下定理：

定理1 设$K=\boldsymbol{Q}(\sqrt{d})$为二次域，$d$为无平方因子有理整数，则：(1)奇素数$p$在$K$分解如下：

$$pO_K=\begin{cases}\wp^2, \quad \wp=(p,\sqrt{d}), & \text{当}d\equiv 0 \pmod p;\\ \wp_1\wp_2,\wp_i=(p,\sqrt{d}\pm a), & \text{当}d\equiv a^2(\text{mod } p),a\in\boldsymbol{Z}-(0);\\ \wp,\wp=(p), & \text{当}(\frac{d}{p})=-1.\end{cases}$$

(2) 2在K分解如下：

$$2O_K=\begin{cases}\wp^2, \quad \wp=(2,\sqrt{d}) \text{ 或 } (2,\sqrt{d}+1),\\ \qquad\text{分别当 } d\equiv 2 \text{ 或 } 3 \pmod 4;\\ \wp_1\wp_2,\ \wp_i=(2,\frac{1\pm\sqrt{d}}{2}), \text{ 当 } d\equiv 1 \pmod 8;\\ \wp, \quad \wp=(2), \qquad \text{当 } d\equiv 5 \pmod 8.\end{cases}$$

素分解$pO_K=\wp^2$，$\wp_1\wp_2$ ($\wp_1\neq\wp_2$)，$\wp$三种情形分别称为p

在 K 中分歧（Ramification），分裂（Split），惯性（Inertia）. 三种情形下分别记

$$\left(\frac{d}{p}\right)=\begin{cases}0,\\1,\\-1.\end{cases}$$

这称为 **Kronecker 符号**，显然当 $p\neq 2$ 时，这与 Legendre 符号一致. 当 $p=2$ 时，$\left(\frac{d}{2}\right)=1$ 意味着 $d\equiv 1 \pmod 8$，$\left(\frac{d}{2}\right)=-1$ 意味着 $d\equiv 5 \pmod 8$，其余情形（即 $d\equiv 2$ 或 3，亦即判别式 $D(K)\equiv 0 \pmod 4$）均为 $\left(\frac{d}{2}\right)=0$.

3.7.1 多重二次域中的素分解

考虑 2^n 次数域

$$L=\boldsymbol{Q}(\sqrt{d_1},\cdots,\sqrt{d_n}).$$

其中 $d_1,\cdots,d_n$ 是无平方因子有理整数，L 常称为 n 重二次域或 $(2,\cdots,2)$（n 重）型数域. 对于任意的 n，可以确定任一素数 p 在 L 中的分解情形[Zh1]：

$$pO_L=(\wp_1\cdots\wp_g)^e,\qquad efg=2^n.$$

显然 L 有 2^n-1 个. 二次子域 $K_v=\boldsymbol{Q}(\sqrt{d_v})$，$d_v$ 是 $d_i(i\in v)$ 之积的无平方因子部分（v 过 $\{1,\cdots,n\}$ 的非空子集）. 例如 $L=\boldsymbol{Q}(\sqrt{2},\sqrt{3},\sqrt{10})$ 的二次子域共 7 个，$d_v=2,3,10,6,5,30$ 和 15. L 的生成（写法）不是唯一的，例如 d_1 换为 d_1d_2（的无平方因子部分）也可以. 但二次子域集是唯一的，可以用来确定 p 在 L 中的分解情形.

(1) 当 p 为奇素数时，记 $S_p(L)=\prod_v\left(\frac{d_v}{p}\right)$ 为诸 Legendre 符

号$(\frac{d_v}{p})$的形式积，v 过$\{1,\cdots,n\}$的子集(当 $v=\varnothing$ 为空集时，约定 $d_v=1$)．例如，当 $p=3$ 时，对 $L=Q(\sqrt{2},\sqrt{3},\sqrt{10})$，$S_3(L)=(\frac{1}{3})(\frac{2}{3})(\frac{3}{3})(\frac{10}{3})(\frac{6}{3})(\frac{5}{3})(\frac{30}{3})(\frac{15}{3})=1\cdot(-1)\cdot 0\cdot 1\cdot 0\cdot(-1)\cdot 0\cdot 0=1^2\cdot(-1)^2\cdot 0^4$.

按奇素数 p 的分解准形，L 分为 4 类，且可取 $d_1,\cdots,d_n$ 如下表：

分类序号	$((\frac{d_1}{p}),\cdots,(\frac{d_n}{p}))$	$S_p(L)$	e	f	g
C_p^1	$(1,\cdots,1)$	1^{2^n}	1	1	2^n
C_p^2	$(-1,1,\cdots,1)$	$1^{2^{n-1}}\cdot(-1)^{2^{n-1}}$	1	2	2^{n-1}
C_p^3	$(0,1,\cdots,1)$	$1^{2^{n-1}}\cdot 0^{2^{n-1}}$	2	1	2^{n-1}
C_p^4	$(-1,0,1,\cdots,1)$	$(1\cdot(-1))^{2^{n-2}}\cdot 0^{2^n-1}$	2	2	2^{n-2}

(当 $n=1$ 时只有前三类)．例如对于 $p=3$，$L=Q(\sqrt{2},\sqrt{3},\sqrt{10})$属 C_p^4，$e=2$，$f=2$，$g=2$.

(2) 当 $p=2$ 时，记形式积 $S_2(L)=\prod\limits_v[d_v]$，其中$[d_v]$为 d_v 的模 8 剩余．

例如，对 $L=Q(\sqrt{2},\sqrt{3},\sqrt{10})$，$S_2(L)=1\cdot 2\cdot 3\cdot 2\cdot 6\cdot 5\cdot 6\cdot 7=1\cdot 5\cdot 3\cdot 7\cdot 2^2\cdot 6^2$.

按 2 的分解准形 L 分为如下 8 类，且可取 $d_1,\cdots,d_n$ 如下表：

分类序号	$(d_1,\cdots,d_n)\bmod 8$	$S_2(L)$	e	f	g
C_2^1	$(1,\cdots,1)$	1^{2^n}	1	1	2^n
C_2^2	$(5,1,\cdots,1)$	$1^{2^{n-1}}\cdot(5)^{2^{n-1}}$	1	2	2^{n-1}
C_2^3	$(\pm 2,1,\cdots,1)$	$1^{2^{n-1}}\cdot(\pm 2)^{2^{n-1}}$	2	1	2^{n-1}
C_2^4	$(\pm 2,5,1,\cdots,1)$	$1^{2^{n-2}}\cdot(5\cdot(\pm 2)^2)^{2^{n-2}}$	2	2	2^{n-2}
C_2^5	$(E,1,\cdots,1)$	$1^{2^{n-1}}\cdot E^{2^{n-1}}$	2	1	2^{n-1}
C_2^6	$(3,5,1,\cdots,1)$	$1^{2^{n-2}}\cdot(5\cdot 3\cdot 7)^{2^{n-2}}$	2	2	2^{n-2}
C_2^7	$(E,2,1,\cdots,1)$	$1^{2^{n-2}}\cdot(E\cdot 2\cdot 6)^{2^{n-2}}$	4	1	2^{n-2}
C_2^8	$(3,2,5,1,\cdots,1)$	$1^{2^{n-3}}\cdot(5\cdot 3\cdot 7\cdot 2^2\cdot 6^2)^{2^{n-3}}$	4	2	2^{n-3}

其中 $E=3$ 或 7(当 $n=2$(或 1)只分前 5(或 3)类). 当然也可将 C_2^3 与 C_2^5 合并, C_2^4 与 C_2^6 合并. 例如, $L=Q(\sqrt{2},\sqrt{3},\sqrt{10})$ 属于 C_2^8, $e=4$, $f=2$, $g=1$.

对于更一般的次数为素数幂的 Abel 域 L, 也可较明显得到 L 中的素分解情形和 L 的分类, 与上述分类很类似. 不过这要用到更进一步的域的特征等理论.

以上二章用理想论讨论了数域, 为了更进一步研究, 需要赋值论和局部域的理论, 以下两章介绍.

第四章　赋值论与完备化

§4.1　p-adic 数

K. Hensel(1908)首先引入 p-adic 数，推广了实数和复数的(普通)绝对值概念，发展出赋值理论. 它不仅是研究代数数论(特别是类域论)的简捷有力工具，而且在单变量代数函数论，整闭整环和代数几何中均有重要应用.

先从初等数论中解方程说起. 方程

$$x^2 - 2 = 0 \tag{1}$$

在 $\boldsymbol{Z}$ 中显然无解. 但对任一素数 p，可考虑它的模 p^n 同余解 x_{n-1}. 例如取 $p=7$，易知(1)对模 7 有解 $x_0=a_0=3$. 再令 $x_1=a_0+a_1p$，a_1 待定，代入方程(1)(mod7^2)，可得 $x_1=3+7$. 同样可得方程(1)的模 7^3 同余解为 $x_2=3+7+2\cdot 7^2$，模 7^4 解为 $x_3=3+7+2\cdot 7^2+6\cdot 7^3$，等等. 故对任意 $n\geqslant 0$，可得方程(1)(mod p^n)的解

$$x_{n-1} = a_0 + a_1p + \cdots + a_{n-1}p^{n-1},\quad (0\leqslant a_i < p).$$

而且 x_{n-1}与 x_{n-2}的前面各项均相同，只多出一项 $a_{n-1}p^{n-1}$. 当 n 很大的时候，我们有一种感觉，好像 x_{n-1}"差不多"就是原方程的解(如果对模 p 的一万次方时 x_{n-1}满足方程的话，在多数"实

用"情形下，x_{n-1}可视为事实上的解了）. 而且 n 可以任意地大，解 x_{n-1}可以任意地"精确"下去. 这就引入两点想法：

(1) n 越大，p^n 越显得微不足道，似应给它定义（赋以）一个微小的"值".

(2) 序列 $x_0, x_1, \cdots, x_n, \cdots$似在趋于一极限值.

这引导我们作如下定义.

定义 1 (1) 对有理数 $p^n b/a$ $(a,b,n\in \mathbf{Z}; p\nmid a, p\nmid b)$，定义其 **p-adic 赋值**为

$$|p^n b/a|_p = \left(\frac{1}{p}\right)^n.$$

(2) 无限级数 $a_0+a_1p+a_2p^2+\cdots(0\leqslant a_i<p)$称为 **p-adic 整数**，全体记为 $\boldsymbol{Z}_p$. $\boldsymbol{Z}_p$ 的分式域记为 $\boldsymbol{Q}_p$，其中元素称为 **p-adic（有理）数**，即形如以下的无限级数：

$a_{-m}p^{-m}+\cdots+a_{-1}p^{-1}+a_0+a_1p+a_2p^2+\cdots$

(m 为任一正整数，$0\leqslant a_i<p$).

例如 $x=3+7+2\cdot 7^2+6\cdot 7^3+\cdots\in \mathbf{Z}_7$，$|x|_7=1$. 再如 $y=2\cdot 7^4+2\cdot 7^5+\cdots\in \mathbf{Z}_7$，$|y|_7=(1/7)^4$. 而 $z=2\cdot 7^{-3}+2\cdot 7^{-2}+3\cdot 7^{-1}+3+2\cdot 7+3\cdot 7^2+\cdots\in \boldsymbol{Q}_7$，$|z|_7=(1/7)^{-3}=7^3$.

有了定义 1，就可以说 $x^2-2=0$ 在 $\boldsymbol{Q}_7$ 中有（7-adic 数）解：$x=3+7+2\cdot 7^2+6\cdot 7^3+\cdots$. 有时记此解为 $\sqrt{2}\in \boldsymbol{Q}_7$.

注意 $\mathbf{Z}\subset \mathbf{Z}_p$，$\boldsymbol{Q}\subset \boldsymbol{Q}_p$. 若记 $\mathbf{Z}'$ 为 $\mathbf{Z}$ 对 (p) 的局部化环 $(\mathbf{Z}-(p))^{-1}\mathbf{Z}$，则有

$$\boldsymbol{Z}\subset \boldsymbol{Z}'\subset \boldsymbol{Z}_p.$$

事实上，对任一 $b/a\in \mathbf{Z}'$，由 $p\nmid a$ 知

$$a = a_0 + a_1p + \cdots + a_tp^t,\ (a_0 \neq 0, 0 \leqslant a_i < p).$$

故有 $a_0'\in \mathbf{Z}$ 使 $a_0'a_0\equiv 1 \pmod p$. 故

$$a'_0 a = 1 + b_1 p + \cdots + b_t p^t,\ (0 \leqslant b_i < p).$$

$$\frac{1}{a} = \frac{a'_0}{a'_0 a} = a'_0 (1 + b_1 p + \cdots + b_t p^t)^{-1}$$

$$= a'_0 (1 - (b_1 p + \cdots + b_t p^t) - (b_1 p + \cdots + b_t p^t)^2 - \cdots)$$

$$\in \mathbf{Z}_p.$$

最后等号是由于对形式幂级数乘法有

$$(1+x)(1-x-x^2-\cdots)=1.$$

故知 $b/a \in \mathbf{Z}_p$，$\mathbf{Z}' \subset \mathbf{Z}_p$. 上述事实上也证明了

命题 1 设 $a = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbf{Z}_p$. $(0 \leqslant a_i < p)$，则当且仅当 $a_0 \neq 0$ 时，a 在 $\mathbf{Z}_p$ 中可逆.

命题 2 $\mathbf{Z}_p$ 的全部真理想为 (p)，(p^2)，(p^3)，$\cdots$(其中 $(a) = a\mathbf{Z}_p$).

证明 设 I 为 $\mathbf{Z}_p$ 的非 0 理想，不妨设

$$a = a_m p^m + a_{m+1} p^{m+1} + \cdots \quad (a_m \neq 0)$$

是 I 中含有 p 的最低次幂项的元素(之一). 于是

$$a = p^m a', \qquad a' = a_m + a_{m+1} p + \cdots.$$

由命题 1 知 a' 在 $\mathbf{Z}_p$ 中可逆，即存在 $b \in \mathbf{Z}_p$ 使 $a'b = 1$. 故 I 含 $ab = p^m a' b = p^m$，即知 $I = (p^m)$. □

还显然有

$$\mathbf{Z}_p / p\mathbf{Z}_p = \mathbf{Z}' / p\mathbf{Z}' = \mathbf{Z} / p\mathbf{Z}.$$

习　题

1. 求 $3x=2$ 的 5-adic 解(至模 5^5).
2. 求 $x^2=7$ 的 3-adic 解(至模 3^5).

§4.2 赋　值

定义 1　域 K 的一个赋值（或称绝对值，valuation 或 absolute value），即是 K 到实数域 $\boldsymbol{R}$ 的一个映射 $\varphi: x \longmapsto |x|_v$，且满足以下三个条件（对任意 $x, y \in K$）：

V1（正定性）．$|x|_v > 0$（当 $x \neq 0$），$|0|_v = 0$.

V2（积性）．$|xy|_v = |x|_v |y|_v$.

V3（三角形不等式）．$|x+y|_v \leqslant |x|_v + |y|_v$.

如果赋值 φ 还满足比 V3 更强的下述条件：

V3′（超三角形不等式）．$|x+y|_v \leqslant \max\{|x|_v, |y|_v\}$，则称 φ 为非阿基米德的（non－archimedean），否则称 φ 为阿基米德的．上述赋值 φ 也记为 $|\ \ |_v$ 或称为 v，有时也记 $|x|_v = |x| = \varphi(x)$.

赋值的积性（即 V2）说明 $\varphi: K^* \longrightarrow \boldsymbol{R}^*$ 是群的同态．由此立刻知道 $|1| = 1$，$|a^{-1}| = |a|^{-1}$，$|b/a| = |b|/|a|$，$|-1| = 1$，$|-a| = |a|$．而且若 ζ 为单位根则 $|\zeta| = 1$（由于 $|\zeta|^m = |\zeta^m| = 1$）.

例 1（平凡赋值）　令 $|x|_v = 1$（对所有 $0 \neq x \in K$），则得一赋值，称为平凡赋值，显然是非阿基米德赋值．当 K 为有限域时，K 只有平凡赋值，这是因为 K 的非 0 元均为单位根．今后总设我们讨论的赋值不是平凡的.

例 2（无限赋值）　当 $K = \boldsymbol{R}$ 或 $\boldsymbol{C}$ 时，普通绝对值即是一个

赋值，称为无限或无穷赋值，记为$|\ \ |_\infty$，是阿基米德赋值.

例 3(p-adic 赋值)　考虑有理数域$\boldsymbol{Q}$. 如上节，固定素数 p，对有理数 $p^n b/a$ ($p\nmid ab$)，令

$$|p^n b/a|_p=(1/p)^n,$$

则$|\ \ |_p$是$\boldsymbol{Q}$的一个赋值，称为 p-adic 赋值，显然是非阿基米德赋值.

例 4(有理函数域的赋值)　设 F 为任一域，X 是不定元，$F[X]$是 F 上的多项式(形式)环. $F[X]$的分式域 $k=F(X)$称为有理式(形式)域或有理函数域. $F[X]$与 $F(X)$的关系类似于 $\mathbf{Z}$ 与 $\boldsymbol{Q}$ 的关系.

(1) 设 $p=p(X)$是 $F[X]$中首一不可约多项式，于是 $F(X)$中每个有理式可表为

$$f=p^n h/g\quad (p\nmid gh,\ n\in\mathbf{Z},\ f,g\in F[X]),$$

令

$$|f|_p=\left(\frac{1}{e}\right)^n,$$

则$|\ \ |_p$是 $F(X)$中一赋值，称为 $p(X)$-adic 赋值.(上式中 $1/e$ 也可换为任一常数 $\varepsilon(0<\varepsilon<1)$). 特别当 $F=\boldsymbol{C}$ 时，必有 $p(X)=X-c$，可知 n 就是 f 在点 $c\in\boldsymbol{C}$ 的阶，所以复平面上每一个点(位置)c 都对应一个$(X-c)-$adic 赋值.(因此赋值也常称作"位").

(2) 每个 $f\in F(X)$可表为

$$f(X)=\frac{b_nX^n+\cdots+b_1X+b_0}{a_mX^m+\cdots+a_1X+a_0},\quad (a_m,b_n\neq 0).$$

令

$$|f|_\infty=\left(\frac{1}{e}\right)^{m-n},$$

则易知$|\ \ |_\infty$是$F(X)$的赋值，称为无限(或无穷)赋值，它也是非阿基米德赋值(注意，这一点与Q的无限赋值不同!). 当然上述$1/e$也可换为任一小于1的正常数ε.

上述$f(X)$可改写为

$$\begin{aligned}f(X)&=\frac{X^n}{X^m}\cdot\frac{b_n+b_{n-1}\left(\frac{1}{X}\right)+\cdots+b_0\left(\frac{1}{X}\right)^n}{a_m+a_{m-1}\left(\frac{1}{X}\right)+\cdots+a_0\left(\frac{1}{X}\right)^m}\\&=\left(\frac{1}{X}\right)^{m-n}h\left(\frac{1}{X}\right)\Big/g\left(\frac{1}{X}\right),\end{aligned}$$

与本例(1)中$p(X)$-adic赋值相比可知，此处的无限赋值实即为$\left(\frac{1}{X}\right)$-adic赋值(注意$h\left(\frac{1}{X}\right)$和$g\left(\frac{1}{X}\right)$均不含"因子"$\frac{1}{X}$). 因为$\frac{1}{X}$的零点位在$\infty$，故$\left(\frac{1}{X}\right)$-adic赋值称为无限赋值. 通过变量代换$Y=\frac{1}{X}$，$F(X)=F\left(\frac{1}{X}\right)=F(Y)$，可知$\left(\frac{1}{X}\right)$-adic赋值即为$Y$-adic赋值.

例5($\wp$-adic赋值) 设K为数域，$\wp$为其非0素理想，K中任一数α生成的分式理想可表为

$$(\alpha)=\wp^s I/J \qquad (\wp\nmid IJ),$$

其中I,J为与$\wp$互素的整理想，定义α的$\wp$-adic赋值为

$$|\alpha|_\wp=\left(\frac{1}{p^{1/e}}\right)^s,$$

这里$e=e(\wp|p)$是$\wp$的分歧指数，$p=\wp\cap\mathbf{Z}$. 有时也把上述$p^{1/e}$换为$N\wp=\#(O_K/\wp)$，而定义α的另一(标准化的)$\wp$-adic赋

值为

$$\| a \|_{\wp} = \left(\frac{1}{N\wp} \right)^{s}.$$

注意

$$|p|_{\wp} = \left(\frac{1}{p^{1/e}} \right)^{e} = \frac{1}{p} = |p|_{p},$$

故$|\ \ |_{\wp}$在$\boldsymbol{Q}$上限制为$|\ \ |_{p}$.

域K的每个赋值$\varphi: x \longmapsto |x|_v$决定了$K$上一个距离函数$d:(x,y) \longmapsto |x-y|_v$,即定义$x$与$y$的距离为

$$d(x,y) = |x-y|_v,$$

这就决定了域K上的一个度量拓扑,记为T_φ或T_v. 此度量拓扑的基是开球全体(即开集均为开球的并),$a \in K$的基本邻域系就是以a为中心的开球全体:

$$U(a,\varepsilon) = U_\varphi(a,\varepsilon) = \{x \in K \mid |x-a|_v < \varepsilon\}.$$

显然,序列$\{x_n\}$在拓扑T_φ下趋于0当且仅当$|x_n|_v$趋于0. 映射φ对拓扑T_φ是一致连续的(由$\varphi(a) \leqslant \varphi(a-b)+\varphi(b)$及$\varphi(b) \leqslant \varphi(b-a)+\varphi(a)$易知$|\varphi(a)-\varphi(b)|_\infty \leqslant \varphi(a-b)$). K对T_φ为拓扑域.

如果两个赋值$|\ \ |_1$和$|\ \ |_2$所决定的拓扑T_1和T_2相同,则称此二赋值是**等价的**. 例如,两赋值φ和φ^λ显然是等价的,这里λ为正实数,

$$\varphi^\lambda(x) = \varphi(x)^\lambda.$$

事实上,T_φ和$T_{\varphi\lambda}$的基本邻域系$\{U_\varphi(a,\varepsilon)\}$和$\{U_{\varphi\lambda}(a,\gamma)\}$显然是等价的:对任意$U_\varphi(a,\varepsilon)$,显然有$U_{\varphi\lambda}(a,\varepsilon^\lambda) \subset U_\varphi(a,\varepsilon)$,反之亦然. 所以这两个基本邻域系所决定的拓扑$T_\varphi$和$T_{\varphi\lambda}$是相同的.

这就引起一个问题:若φ是K的赋值,λ为任一正实数,φ^λ是否为赋值? 当φ是非阿基米德赋值时,φ^λ显然是赋值,这由超

三角形不等式 V3′可知．然而当 φ 是阿基米德赋值时，φ^2 却未必是赋值．例如取 φ 为 $\boldsymbol{Q}$ 的普通绝对值，φ^2 便不满足 V3，因为 $\varphi^2(3+3)=\varphi((3+3)^2)3^2+2\cdot 3^3+3^2=4\cdot 3^2=4\varphi^2(3)$．E. Artin 在〔$A1$〕(1967)中建议扩充赋值的定义，使得 φ^2 总为赋值．我们现作讨论．

4.2.1 一般赋值

设域 K 到 $\boldsymbol{R}$ 的映射 φ: $x\longmapsto|x|_v=\varphi(x)$ 满足定义 1 中的 V1(正定性)和 V2(积性)，若 φ 还满足(对任意 $x,y\in K$)：

V3(A)．$|x+y|_v\leqslant c(|x|_v+|y|_v)$

或

V3(M)．$|x+y|_v\leqslant C\max\{|x|_v,|y|_v\}$

(其中 c,C 为某固定正实数)，则 φ 称为(**一般**)**赋值**，也分别称为 A-赋值和 M-赋值．(相应地，满足定义 1 的赋值有时称为古典赋值)．

满足 V3(A)和 V3(M)的最小的 c 和 C 分别记为

$$c_0=|\varphi|,\quad C_0=\|\varphi\|,$$

称为 φ 的 A-范和 M-范．取 $y=0$ 可知 $c_0\geqslant 1,C_0\geqslant 1$．

定理 1 设 φ: $K\to\boldsymbol{R}$ 满足 $V1$ 和 $V2$，则 $V3(A)$ 与 $V3(M)$ 等价．且当 φ 满足 $V3(A)$ 或 $V3(M)$ 时有：

(1) $c_0=1$ 当且仅当 $C_0\leqslant 2$ (此时 φ 满足 $V3$ 即三角形不等式)．

(2) $c_0=\frac{1}{2}C_0$ (当 $c_0>1$ 或 $C_0\geqslant 2$)．

(3) $C_0=\varphi(2)$ (当 φ 是阿基米德赋值)或 1(否则)．对一般的 φ 总有 $C_0=\max\{\varphi(1),\varphi(2)\}$．

引理 1　设 $\varphi: K \to \boldsymbol{R}$ 满足 V1 和 V2.

（Ⅰ）若 φ 满足 V3(A)，则 φ 满足 V3(M)（对于 $C=2c$）.

（Ⅱ）若 φ 满足 V3(M)，则 φ 满足 V3(A)（对于 $c=1$（当 $C\leqslant 2$），或 $c=C/2$（当 $C\geqslant 2$））.

引理 1 证明　（Ⅰ）由 $|x+y|_v\leqslant c(|x|_v+|y|_v)\leqslant c(2\max\{|x|_v,|y_v|\}=2c\max\{|x|_v,|y|_v\}$ 即知.

（Ⅱ）$(\varphi(x+y))^n=\varphi((x+y)^n)=\varphi(\sum_i C_n^i x^{n-i}y^i)$. 注意由 V3(M)知

$$\varphi(x_1+\cdots+x_4)\leqslant C^2\max_i\varphi(x_i),$$

由归纳法可知，当 $m=2^r$ 时，

$$\varphi(x_1+\cdots+x_m)\leqslant C^r\max_i\varphi(x_i),\qquad (*)$$

当 $m<2^r$ 时，我们可令 $x_{m+1}=\cdots=x_{2^r}=0$，故（*）式仍然成立. 现设 $2^{r-1}<n+1\leqslant 2^r$，则知

$$\begin{aligned}\varphi(x+y)^n&\leqslant C^r\max_i\varphi(C_n^i x^{n-i}y^i)\\&=C^r\varphi(C_n^j)\varphi(x^{n-j})\varphi(y^j)\\&<C^r\varphi(C_n^j)(C_n^j)^{-1}\sum_{i=0}^n C_n^i\varphi(x)^{n-i}\varphi(y)^i\\&=C^r\varphi(C_n^j)(C_n^j)^{-1}(\varphi(x)+\varphi(y))^n,\end{aligned}$$

其中第一个等号是由于我们设当 $i=j$ 时取得最大值；然后增加了 n 项. 上式两边开 n 次方，再令 $n\to\infty$，则有如下形式不等式：

$$\varphi(x+y)\leqslant S(\varphi(x)+\varphi(y)),$$

其中 S 是 $(\varphi(C_n^j)/C_n^j)^{1/n}$ 的上极限. 记 $t=\log_2 C_n^j$，则 $C_n^j=2^t\leqslant 2^{t_0}$，其中 t_0 是满足 $t_0\geqslant t$ 的最小正整数，于是由（*）式及 $\varphi(C_n^j)=\varphi(1+\cdots+1)$ 知

$$\varphi(C_n^j)\leqslant C^{t_0}\varphi(1)<C\cdot C^t,$$

$$\varphi(C_n^j)/C_n^j<CC^t/2^t=C(C/2)^t. \qquad (**)$$

(i) 当 $C\leqslant 2$ 时,由($**$)式知 $\varphi(C_n^j)/C_n^j\leqslant C$,故 $S=1$. 引理得证.

(ii) 当 $C\geqslant 2$ 时,$C_n^j=2^t$ 的最大值当 $j=n/2$ 时取到(不妨设 n 为偶数). 故

$$C_n^j\leqslant C_n^{n/2}=\frac{n!}{((n/2)!)^2}=\frac{\sqrt{2\pi n}(n/e)^n e^{\theta/12n}}{(\pi n)(n/2e)^n e^{\theta_1/12n}}$$
$$=\sqrt{2/n\pi}\,2^n e^{(\theta-\theta_1)/12n}<2^{n+1}.$$

(当 n 充分大时,其中 $0<\theta,\theta_1<4$). 故总有

$$t\leqslant n+1.$$

由($**$)式即知 $\varphi(x+y)^n<C^{r+2}(C/2)^n(\varphi(x)+\varphi(y))^n$,开 n 方令 $n\to\infty$ 即得 $\varphi(x+y)\leqslant(C/2)(\varphi(x)+\varphi(y))$. □

定理 1 证明 由引理 1 即知 V3(A)与 V3(M)等价. (1)若 $c_0=1$,即 V3(A)对 $c_0=1$ 成立,由引理 1(Ⅰ)知 V3(M)对 $C=2c_0=2$ 成立,故 $C_0\leqslant 2$. 反之若 $C_0\leqslant 2$,即 V3(M)对 $C_0\leqslant 2$ 成立,则由(Ⅱ)可知 V3(A)对 $c=1$ 成立,即 $c_0=1$. 定理 1(1)也说明 $c_0>1$ 当且仅当 $C_0>2$. (2)由 V3(M)对 $C_0>2$ 成立可知 V3(A)对 $c=C_0/2>1$ 成立,故 $c_0\leqslant C_0/2$. 反之,由 V3(A)对 $c_0>1$ 成立可知 V3(M)对 $C=2c_0$ 成立,故 $C_0\leqslant 2c_0$,即知 $C=2c_0$.

(3) 若 φ 为非阿基米德赋值,则 $\varphi(2)=\varphi(1+1)\leqslant\max\{\varphi(1),\varphi(1)\}=1$,$\varphi(1)=1=C_0$. 现设 φ 为阿基米德赋值,于是 K 的特征为 0,可设 $\boldsymbol{Q}\subset K$. φ 在 $\boldsymbol{Q}$ 上的限制 ψ 为 $\boldsymbol{Q}$ 的阿基米德赋值,故必有 $\varphi(a)=|a|_\infty^\lambda$(对任意 $a\in\boldsymbol{Q}$,λ 为某正数). 这是 §4.3 定理 1,我们先引用. 由 $2^n=(1+1)^n=\sum\limits_j C_n^j$ 可知 $\varphi(C_n^j)=$

$(C_n^j)^\lambda \leqslant 2^{n\lambda}$. 故由上述引理 1(Ⅱ)的证明可知,对任意 $x,y\in K$,有

$$\varphi(x+y)^n \leqslant C'2^{n\lambda}\varphi(x)^{n-j}\varphi(y)^j \leqslant C'2^{n\lambda}(\max\{\varphi(x),\varphi(y)\})^n,$$

两边开 n 次方,令 $n\to\infty$ 知

$$\varphi(x+y)\leqslant 2^\lambda \max\{\varphi(x),\varphi(y)\}.$$

故 $C_0\leqslant 2^\lambda=\varphi(2)=\varphi(1+1)\leqslant C_0\max\{\varphi(1),\varphi(1)\}=C_0$,即知 $C_0=\varphi(2)$. □

显然若 φ 满足 V3(M),即

$$\varphi(x+y)\leqslant C\max\{\varphi(x),\varphi(y)\},$$

则

$$\varphi^\lambda(x+y)=\varphi(x+y)^\lambda = C^\lambda\max\{\varphi^\lambda(x),\varphi^\lambda(y)\}$$

故 φ^λ 也满足 V3(M). 这说明,若 φ 为(一般)赋值,则 φ^λ 也是(一般)赋值(对任意 $\lambda>0$),且

$$\|\varphi^\lambda\|=\|\varphi\|^\lambda.$$

由此也知 $|\varphi^\lambda|=2^{\lambda-1}|\varphi|^\lambda$.

当 $\|\varphi^\lambda\|>2$ 时,$\psi=\varphi^\lambda$ 不再满足三角形不等式,但仍可定义 x 与 y(对于 ψ)的距离为 $\psi(x-y)$,开球族 $U_\psi(a,\varepsilon)=\{x|\psi(x-a)<\varepsilon\}$ 仍可作为基本邻域系,从而决定 K 的一个拓扑 T_ψ(不再是度量拓扑). 基本邻域系 $\{U_\psi(a,\varepsilon)\}$ 与 $\{U_\varphi(a,\varepsilon)\}$ 显然等价,故 $T_\psi=T_\varphi$. 即 φ 与 φ^λ 等价.

定理 2 设 $|\ \ |_1$ 和 $|\ \ |_2$ 为 K 的两个(一般)赋值,T_1 和 T_2 分别为其决定的拓扑,则以下各命题等价(对任意 $x\in K$):

(1) $|x|_2=|x|_1^\lambda$ (对某固定 $\lambda>0$);

(2) $|\ |_1$ 与 $|\ |_2$ 等价,即 $T_1=T_2$;

(3) T_1 强于 T_2(即 T_2 的开集也是 T_1 的开集);

(4) $|x|_1<1\Rightarrow|x|_2<1$;

(5) $|x|_1 \leqslant 1 \Rightarrow |x|_2 \leqslant 1$,

(6) $\begin{cases} |x|_1 < 1 \Leftrightarrow |x|_2 < 1, \\ |x|_1 > 1 \Leftrightarrow |x|_2 > 1, \\ |x|_1 = 1 \Leftrightarrow |x|_2 = 1. \end{cases}$

证明 (1)⇒(2)：显然．(2)⇒(3)：显然．

(3)⇒(4)：由 $|x|_1<1$ 知 $|x|_1^n \to 0$，故 $x^n \to 0$（T_1 下）．故 $x^n \to 0$（T_2 下），即 $|x^n|_2 \to 0$，$|x|_2<1$．

(4)⇒(5)：取 $b \in K^*$ 使 $|b|_1<1$（因赋值非平凡，故有 b 使 $|b|_1 \neq 1$，从而可设 $|b|_1<1$）．于是若 $|x|_1=1$，则 $|bx^n|_1<1$，故 $|bx^n|_2<1$，$|x|_2<1/|b|_2^{1/n}$（对任意 $n>0$，即知 $|x|_2 \leqslant 1$．同理可知 $|x^{-1}|_2 \leqslant 1$，故 $|x|_2=1$．

(5)⇒(6)：取 $c \in K^*$ 使 $|c|_2<1$．由 $|x|_1<1$ 知 $|x|_1^n \leqslant |c|_1$（对某充分大的 n）．故 $|x^n/c|_1 \leqslant 1$，从而 $|x^n/c|_2 \leqslant 1$．故 $|x^n|_2 \leqslant |c|_2<1$，即知 $|x|_2<1$，(4)成立．再由上述(4)⇒(5)知：若 $|x|_1=1$ 则 $|x|_2=1$．而 $|x|_1>1$ 相当于 $|x^{-1}|_1<1$，从而 $|x^{-1}|_2<1$，$|x|_2>1$．

(6)⇒(1)：取定 $a \in K$ 使 $|a|_1>1$．于是 $|a|_2>1$．令 $\lambda=\log|a|_2/\log|a|_1$．为证(1)，只需要证明对每个 $b \in K^*$，若记 $y_1=\log|b|_1/\log|a|_1$，$y_2=\log|b|_2/\log|a|_2$，则 $y_1=y_2$．设 $r=m/n \in \boldsymbol{Q}$，$n>0$，则 $r=m/n \geqslant y_1 \Leftrightarrow m\log|a|_1 \geqslant n\log|b|_1 \Leftrightarrow |a^m|_1 \geqslant |b^n|_1 \Leftrightarrow |b^n/a^m|_1 \leqslant 1 \Leftrightarrow |b^n/a^m|_2 \leqslant 1 \Leftrightarrow m\log|a|_2 \geqslant n\log|b|_2 \Leftrightarrow m/n \geqslant y_2$．定理 2 获证． □

域 K 的（一般）赋值的一个等价类称为一个**素除子**（prime divisor），也称为一个**位**．由定理 2 可知，φ 所在的素除子恰为

$$P=\{\varphi^\lambda \mid \lambda>0\}.$$

显然，每个素除子 P 中均存在赋值 φ 满足 $\|\varphi\| \leqslant 2$，即满足三角

形不等式．(非)阿基米德赋值构成的素除子称为(非)阿基米德素除子.

4.2.2 非阿基米德赋值

域 K 的非阿基米德赋值 φ: $x \longmapsto |x|_v$ 有独特的性质．令

$$v(x) = -\log |x|_v, \quad (x \in K)$$

则 $v(x)$ 称为 x 的指数赋值(exponential valuation)(log 的底可任意固定)．于是赋值三条件转化为：

V1. $v(0)=\infty$;

V2. $v(xy)=v(x)+v(y)$;

V3′. $v(x+y)\geqslant\min\{v(x),v(y)\}$.

而 v 所在的素除子为 $P=\{\lambda v|\lambda>0\}$. 例如 $\boldsymbol{Q}$ 的 p-adic 赋值对应的指数赋值可取为 v_p:

$$v_p(p^n a/b) = n.$$

命题 1 记号如上，设 $x,y\in K$.

(1) 若 $v(x)\neq v(y)$，则

$$v(x + y) = \min\{v(x),v(y)\}.$$

(即：若 $\varphi(x)\neq\varphi(y)$，则 $\varphi(x+y)=\max\{\varphi(x),\varphi(y)\}$).

(2) 若 $\varphi(x-y)<\varphi(x)$，则 $\varphi(x)=\varphi(y)$.

证 (1) 不妨设 $v(x)>v(y)$. 于是

$$v(y)=v(x+y-x)\geqslant\min\{v(x+y),v(x)\}$$
$$\geqslant\min\{v(x),v(y)\}=v(y).$$

(2) 否则由(1)可知 $\varphi(x-y)=\max\{\varphi(x),\varphi(y)\}\geqslant\varphi(x)$，与所设矛盾.

注意上述(2)说明：当 x 与 y 充分靠近时，二者的赋值相

同. 设 P 是 K 的一个非阿基米德素除子,取其中任一赋值 φ: $x \longmapsto |x|$. 并记其对应的指数赋值为 v,令

$$O=\{x\in K \quad |x|\leqslant 1\}=\{x\in K|v(x)\geqslant 0\},$$
$$\wp=\{x\in K| \quad |x|<1\}=\{x\in K|v(x)>0\},$$
$$U=\{x\in K| \quad |x|=1\}=\{x\in K|v(x)=0\}.$$

显然 O, $\wp$,U 只依赖于 P 而与 φ 的选取无关(定理 2).O 称为在 P 的**赋值环或整数(元)环**,是含幺整环.K 是 O 的分式域(事实上 $K=O\cup O^{-1}$,O^{-1}指 O 的非 0 元之逆集). $\wp$ 称为在 P 的**赋值(素)理想**,是 O 的素理想.U 称为在 P 的**单位群**,是乘法群,是由 O 的可逆元(单位)组成,且 $U=O\cap O^{-1}$. $\wp$ 显然由所有非单位组成. 故 $\wp$ 是 O 的唯一极大理想. 商环

$$\overline{K}=O/\wp$$

是域,称为 K 在 P 的**剩余类域**. 上述定理 2 说明,两个赋值等价当且仅当其赋值素理想相等,或其赋值环相等,也就是说非阿基米德素除子由其素理想唯一决定.

例 6 设 P 是 $\boldsymbol{Q}$ 的 p-adic 素除子,其中指数赋值 $v=v_p$. 对于互素的 $a,b\in\mathbf{Z}$, $v(\frac{b}{a})=v(b)-v(a)>0$ 显然相当于 $p\nmid a, p\mid b$. 故 P 的赋值环

$$O_p=\{\frac{b}{a}\,|\,p\nmid a,\ a,\ b\in\mathbf{Z}\}=\mathbf{Z}'.$$

就是 $\mathbf{Z}$ 在 p 的局部化.P 的赋值理想显然为

$$\wp_p=\{\frac{b}{a}\,|\,p\nmid a,\ p\mid b,\ a,\ b\in\mathbf{Z}\}=p\mathbf{Z}'.$$

就是局部环 $\mathbf{Z}_p$ 的唯一极大理想.

有趣的是,$\mathbf{Z}$ 显然是所有 p-adic 赋值环的交:

$$\mathbf{Z}=\bigcap_p O_p.$$

例 7 设 P 是数域 K 的 $\wp$-adic 素除子，则 P 的赋值环恰为 K 的整数环 A 在 $\wp$ 的局部化 $A_\wp=\{\frac{b}{a}\mid a\notin\wp, a,b\in A\}$. 事实上，$K$ 中任一元素可表为 $\alpha=u\pi^n$（其中 $n\in\mathbf{Z}$，u 为 $A_\wp$ 的单位，$\pi\in\wp-\wp^2$ 是素元）. $\alpha\in A_\wp$ 当且仅当 $n\geqslant 0$，这恰相当于 $|\alpha|_\wp\leqslant 1$，即 $\alpha\in O_p$（注意 $|u|_\wp=1$，这是因为 $u=b/a$，$\wp\nmid a$，$\wp\nmid b$）. 由此也立知 P 的赋值理想恰为 $A_\wp$ 的素理想 $\wp'=\pi A_\wp$.

最后，我们看一下非阿基米德这一名词的意义．若 φ 是非阿基米德赋值，则

$$\varphi(n)=\varphi(1+\cdots\cdots+1)\leqslant\max\{\varphi(1)\}=1,$$

说明 $1+1+1+\cdots\cdots$ 的赋值是有界的（阿基米德曾提出过这样的问题：$1+1+1+1+\cdots\cdots$ 这样不断加下去，是否有界?）. 事实上我们可以证明：

命题 2 赋值 φ 为 K 的非阿基米德赋值当且仅当 $\varphi(n\cdot 1)$ 有界（对任意 $n\in\mathbf{Z}$，其中 1 为 K 中单位元）.

证 只需再证充分性．设 $\varphi(n\cdot 1)$ 有界 M. 由引理 1(**1**) 的证明可知（我们设 $\varphi(x)\geqslant\varphi(y)$）：

$$\begin{aligned}\varphi(x+y)^n&\leqslant C^r\varphi(C_n^i)\max_i\{\varphi(x)^{n-i}\varphi(y)^i\}\\&\leqslant C^rM\varphi(x)^n,\end{aligned}$$

其中 $2^{r-1}<n+1\leqslant 2^r$. 开 n 次方，令 $n\to\infty$，则得

$$\varphi(x+y)\leqslant\varphi(x)=\max\{\varphi(x),\varphi(y)\}.\qquad\square$$

由命题 2 可知，非阿基米德赋值 φ 与阿基米德赋值 ψ 不可能等阶，因为 $\varphi(n)\leqslant 1$ 而 $\psi(n)$ 无界（定理 2）. 还可知 K 上一个赋值是否是阿基米德的，是由 K 的素子域决定的．特征有限

(非 0)的域 K 只能有非阿基米德素除子.

习　题

1. 设 φ 是域 K 的非阿基米德赋值, $a_1, \cdots, a_n \in K$.

(i) 若 $\varphi(a_1) > \varphi(a_i)$ $(i=2,\cdots,n)$, 则

$$\varphi(a_1 + \cdots + a_n) = \varphi(a_1).$$

(ii) 若 $a_1 + \cdots + a_n = 0$, 则至少有两个元素 a_s 和 a_t 使 $\varphi(a_s) = \varphi(a_t) = \max_i \{\varphi(a_i)\}$

2. 有限域上只能有平凡赋值.

§4.3　数域和函数域的赋值

我们已经看到, $\boldsymbol{Q}$ 有一个阿基米德赋值 φ_∞(普通绝对值), 以 ∞ 记它代表的素除子. 此外, 对每个正素数 p, $x = p^n b/a \in \boldsymbol{Q}$, ($p \nmid b$, a, b, $\in \mathbf{Z}$), $\boldsymbol{Q}$ 有一**标准** p-adic **赋值** φ_p:

$$\varphi_p(p^n b/a) = \left(\frac{1}{p}\right)^n.$$

φ_p 代表的素除子记为 p. 注意若 p 与 q 为不同素数, 则素除子 $p \neq q$(由上节定理 2, $\varphi_p(p) < 1$ 而 $\varphi_q(p) = 1$).

定理 1　(1) 有理数域 $\boldsymbol{Q}$ 的全部非平凡且互不相同的素除子恰为

$$M_Q = \{\infty, 2, 3, 5, 7, \cdots\cdots, p, \cdots\},$$

即无限素除子 ∞ 和 p-adic 素除子全体.

(2) (乘积公式). 对任一非零 $a \in \boldsymbol{Q}$ 总有

$$\prod_{\varphi_p \in M_Q} \varphi_p(a) = 1.$$

证明 (1) 设 P 是 Q 的非阿基米德非平凡素除子，任取其中一赋值 φ. 考虑 P 的(赋值)素理想 $\wp$ 与 $\mathbf{Z}$ 的交 $I=\{n\in\mathbf{Z}|\varphi(n)<1\}$. 显然 I 为 $\mathbf{Z}$ 的素理想且非 0(因 P 非平凡)非 $\mathbf{Z}$(因 $\varphi(1)=1$). 故 $I=p\mathbf{Z}$, p 为某素数. 任一整数可写成 $n=n'p^s$, $(n',p)=1$. 因 $n'\notin p\mathbf{Z}$，故 $\varphi(n')=1$(注意对任一整数 m 均有 $\varphi(m)=\varphi(1+\cdots+1)\leqslant\varphi(1)=1$). 故 $\varphi(n)=\varphi(p)^s$. 由 $\varphi(p)<1$ 知 $\varphi(p)=\left(\frac{1}{p}\right)^{\lambda}(\lambda>0)$，故 $\varphi(n)=\left(\frac{1}{p}\right)^{s\lambda}=\varphi_p(n)^{\lambda}=\varphi_p^{\lambda}(n)$. 故 $\varphi=\varphi_p^{\lambda}$(因为 φ 由其在 $\mathbf{Z}$ 上值决定).

再设 P 是 Q 的阿基米德素除子，取其中一古典赋值 φ(即满足 $\|\varphi\|\leqslant 2$). 任意固定 $m,n>1$，对任意 t 令

$$m^t=a_0+a_1n+\cdots\cdots+a_sn^s\ (0\leqslant a_i<n, a_s\neq 0).$$

于是 $n^s\leqslant m^t$, $s\leqslant t(\log m/\log n)$. 由 $\varphi(a_i)\leqslant a_i<n$ 可知

$$\begin{aligned}\varphi(m^t)&\leqslant\varphi(a_0)+\varphi(a_1)\varphi(n)+\cdots+\varphi(a_s)\varphi(n)^s\\&\leqslant n(1+\varphi(n)+\cdots+\varphi(n)^s)\\&\leqslant n(s+1)M^s.\qquad(\text{其中 } M=\max\{1,\varphi(n)\})\end{aligned}$$

故

$$\varphi(m^t)\leqslant n\left(1+t\frac{\log m}{\log n}\right)M^{t\log m/\log n}.$$

开 t 次方后令 $t\to\infty$ 则得

$$\varphi(m)\leqslant\max\{1,\varphi(n)\}^{\log m/\log n}.$$

我们断言 $\varphi(n)>1(\forall n>1)$，否则若有 $n>1$ 使 $\varphi(n)\leqslant 1$，则由上述不等式知 $\varphi(m)\leqslant 1(\forall m\in\mathbf{Z})$，这与 φ 是非阿基米德的矛盾. 于是知不等式即为

$$\varphi(m)^{1/\log m}\leqslant\varphi(n)^{1/\log n}.$$

由于 m 和 n 的对称性，知

$$\varphi(m)^{1/\log m}=\varphi(n)^{1/\log n}=e^{\lambda} \qquad (\forall\ m,n>1, \text{某 } \lambda>0).$$

故 $\varphi(n)=n^{\lambda}(\forall\ n>1)$. 从而对任意整数 n 有 $\varphi(n)=|n|_{\infty}^{\lambda}=\varphi_{\infty}^{\lambda}(n)$，从而 $\varphi=\varphi_{\infty}^{\lambda}$(因 φ 由其在 $\boldsymbol{Z}$ 上值决定).

(2) 注意对 $a\neq 0\in\boldsymbol{Q}$，几乎对所有(即除有限个之外)的 $p\in M_{\boldsymbol{Q}}$有 $v_p(a)=0$，$\varphi_p(a)=1$. 故乘积事实上是有限的. 而为了证明，只要证明乘积中每个素数 q 的幂为 1，这由 $\varphi_{\infty}(q)=q$，$\varphi_q(q)=\frac{1}{q}$，$\varphi_p(q)=1$(当 $p\neq q$)即知. □

与 $\boldsymbol{Q}$ 的情形类似，我们可以决定有理函数域 $F(X)$的全部素除子. 首先回忆，由 §4.2 例 4 知，$F(X)$有 $p(X)$-adic 赋值和无限赋值，它们决定的素除子分别记为 $p(X)$和∞(其中 $p(X)$是首一不可约多项式). 无限赋值也可看作$(\frac{1}{X})$-adic 赋值.

定理 2 域 F 上有理函数域 $F(X)$的在 F 上平凡的素除子集为

$$M=\{p(X),\infty \mid p(X)\text{为 } F[X]\text{中首一不可约多项式}\}.$$

而且对任一 $f(X)\in F(X)$有

$$\prod_{P\in M}\|f(X)\|_{P}=1. \qquad (\text{乘积公式})$$

其中 $\|\ \|_P$ 为 P 中标准赋值，即

$$\|p(X)\|_{p(x)}=e^{-\deg p(x)},$$

$$\|g(X)\|_{\infty}=e^{\deg g(x)},$$

其中对有理式 h/g 记 $\deg(h/g)=\deg h-\deg g$.

证明 设 P 为 $F(X)$的素除子，$\varphi=|\ \ |$为 P 中一赋值.

(1) 设$|X|\leqslant 1$，即 $X\in O_P$ (P 的赋值环)，于是 $F[X]\subset O_P$.

设 P 的赋值理想 $\wp$ 与 $F[X]$ 的交为 I，则 I 为素理想（因 $\wp$ 素），且 $I\neq 0$（否则说明对 $0\neq g\in F[X]$ 有 $g\notin\wp$ 即 $|g|=1$，从而对 $\frac{h}{g}\in F(X)$ 有 $|h/g|=|h|/|g|=1$，与 P 非平凡矛盾）. 故 $I=(p(X))$，$p(X)$ 为首一不可约多项式．对任一 $g(X)\in F[X]$，若 $p(X)\nmid g(X)$ 则 $g(X)\notin I$，故 $g(X)\notin\wp$，从而 $1/g(X)\in O_P$. 这就证明 $p(X)$-adic 赋值的赋值环 $O_{p(X)}=\{h/g\mid p\nmid g\}\subset O_P$. 由上节定理 2(5)知 P 中赋值与 $p(X)$-adic 赋值等价.

(2) 设 $|X|>1$，即 $|X^{-1}|<1$，$X^{-1}\in\wp$（赋值理想）. 记 $X^{-1}=Y$，于是 $F(X)=F(Y)$. $Y\in\wp\subset O_P$，故 $F[Y]\subset O_P$. 同情形(1)一样知道 $\wp\cap F[Y]=I=(Y)$（因为 Y 不可约）. 故 P 的赋值环为

$$O_P=\{\frac{h(Y)}{g(Y)}|Y\nmid g(Y)\}=O_\infty.$$

即知 P 为无限素除子.

从赋值理想的不同易知 M 中的素除子互异.

再看乘积公式．非零 $f\in F(X)$ 可表为

$$f=cp_1(X)^{n_1}\cdots\cdots p_r(X)^{n_r},$$

其中 $c\in F$，$n_i\in\mathbf{Z}$，p_i 是 $F[X]$ 中首一不可约多项式．于是

$$\prod_P\|f\|_P=\|f\|_\infty\|p_1(X)\|_{p_1}^{n_1}\cdots\cdots\|p_r(X)\|_{p_r}^{n_r}$$
$$=e^{\deg f}e^{-n_1\deg p_1}\cdots\cdots e^{-n_r\deg p_r}=1.$$
□

设域 $F\subset E$，ψ 是 E 的一个赋值（注意 ψ 是到 $\mathbf{R}$ 的一个映射）. 则限制 $\varphi=\psi|_F$ 显然是 F 的赋值，φ 称为 ψ 的**限制赋值**，而 ψ 称为 φ 的**延拓赋值**．记 Q 为 ψ 所在的 E 的素除子，因 $\psi^\lambda|_F=(\psi|_F)^\lambda$，故 Q 中全部赋值在 F 的限制恰构成 F 的一个素除子 P，即 Q 与 P 的赋值间 1∶1 对应．我们也称 P 为 Q 的**限制**，Q 为 P 的**延拓**，而记为 $(E,Q)\supset(F,P)$.

赋值延拓和限制的概念可以稍作推广．如果 $\mu: F\to E$ 是域的嵌入映射，ψ 是 E 的赋值，则 $\psi^{\mu}=\psi\circ\mu$ 是 F 的赋值．我们也称 ψ^{μ} 是 ψ 的限制(经过 μ)，ψ 是 ψ^{μ} 的延拓(经过 μ)．称 ψ 所在素除子 Q 是 ψ^{μ} 所在素除子 P 的延拓，P 是 Q 的限制，记为 $(E,Q,\mu)\supset(F,P)$．由此知 E 的素除子集 M_E 到 F 的素除子集 M_F 中有限制映射 $\mu^*: M_E\to M_F$，$Q\to P=Q\mid_F$．

如果 E/F 为代数扩张，则 F 的平凡素除子 P 到 E 上的延拓 Q 只能是平凡素除子．事实上，若 Q 非平凡，则存在 $\alpha\in E$，$\psi\in Q$ 使 $\psi(\alpha)>1$．而 α 应满足一方程 $\alpha^n+a_1\alpha^{n-1}+\cdots\cdots+a_{n-1}\alpha+a_n=0(a_i\in F)$．但 $\psi(\alpha^n)>\psi(\alpha^{n-i})=\psi(a_i\alpha^{n-i})(1\leqslant i\leqslant n)$，与上式矛盾．(但应注意，对于超越扩张 E/F，F 的平凡赋值在 E 上可有非平凡的延拓)．

定理 3 设 K 为数域，则 K 的全部互不相同的非平凡素除子为

$$M_K=\{\infty_1,\cdots,\infty_r,P_1,P_2,\cdots\cdots\}.$$

其中 ∞_i 是阿基米德素除子，是 $\boldsymbol{Q}$ 的无限素除子 ∞ 的延拓 $(1\leqslant i\leqslant r)$；$P_j$ 为 $\wp_j$-adic(赋值决定的)素除子，$\wp_j$ 为 K 的不同素理想．(j=1,2,……)．(以后可证明 $r=r_1+r_2$，r_1 和 $2r_2$ 分别为 K 到 $\boldsymbol{C}$ 的实和虚嵌入个数)．

证明 设 $\wp$ 是 K 的素理想，$\psi_\wp$ 是 $\wp$－adic 赋值．设 $pZ=\wp\cap\boldsymbol{Z}$，则 $\psi_\wp$ 在 $\boldsymbol{Q}$ 的限制 φ 为 p—adic 赋值，这是因为 φ 的赋值理想为 $p\boldsymbol{Z}$(对 $a\in\boldsymbol{Z}$，$\psi_p(a)<1\Leftrightarrow a\in pZ$)．故 $\wp$ 定义的素除子 P 是 $\boldsymbol{Q}$ 的素除子 p 的延拓．而且若 K 的素理想 $\wp_1\neq\wp_2$，它们决定的素除子 P_1 与 P_2 也不同(因为 P_1 与 P_2 的赋值环(即局部化环)$A_{\wp_1}\neq A_{\wp_2}$)．

反之，设 φ 是 $\boldsymbol{Q}$ 的 p—adic 赋值，ψ 是 φ 到 K 的延拓. 设 O 是 ψ 的赋值环，$\wp_\psi$ 是 ψ 的赋值素理想，则 $\wp=\wp_\psi\cap A$ 是 K 的非 0 素理想(A 表示 K 的整数环)($\wp_\psi\cap A\supset\wp_\psi\cap\boldsymbol{Z}=p\boldsymbol{Z}$ 非 0). 我们要证明 ψ 即为 $\wp$—adic 赋值，这只要证明 $O=A_\wp$ 即可($A_\wp$ 为 A 在 $\wp$ 的局部化).

首先说明 $A\subset O$：任一 $\alpha\in A$ 满足一个整性方程.

$$\alpha^n+a_{n-1}\alpha^{n-1}+\cdots\cdots+a_1\alpha+a_0=0,\ (a_i\in\boldsymbol{Z})$$

故 $\psi(\alpha)^n=\psi(\alpha^n)=\psi(a_{n-1}\alpha^{n-1}+\cdots\cdots+a_0)\leqslant\psi(a_s\alpha^s)\leqslant\psi(\alpha)^s$，其中 $0\leqslant s\leqslant n-1$，$\psi(a_s\alpha^s)=\max\limits_i\{\psi(a_i\alpha^i)\}$. 这即说明 $\psi(\alpha)\leqslant1$，$\alpha\in O$.

再证 $A_\wp=O$：若 $b/a\in A_\wp$，$a,b\in A$，$a\notin\wp$，则 $\psi(b/a)=\psi(b)/\psi(a)\leqslant1$(因 $\psi(b)\leqslant1$，$\psi(a)\geqslant1$)，故 $b/a\in O$. 即知 $A_\wp\subset O$. 另一方面，若 K 中元 $\beta\notin A_\wp$，则 $\beta=u\pi^{-r}$(其中 $\pi\in\wp$，$r>0$，u 是 $A_\wp$ 的单位). 显然 $\psi(u)=1$(因 $u\in A_\wp\subset O$ 知 $\psi(u)\leqslant1$，因 $u^{-1}\in A_\wp$ 知 $\psi(u^{-1})\leqslant1$)，$\psi(\pi)<1$(因 $\pi\in\wp\subset\wp_\psi$)，故 $\psi(\beta)>1$，$\beta\notin O$. 即知 $A_\wp=O$，ψ 为 $\wp$—adic 赋值. □

如何具体求出 $\boldsymbol{Q}$ 的素除子到 K 的延拓呢？以 ∞ 为例，可将 K 嵌入到复数域 $\boldsymbol{C}$ 中，从而将 $\boldsymbol{C}$ 的赋值(即普通绝对值)诱导到 K 上. 详言之，可设 $K=\boldsymbol{Q}(\alpha)$，设 α 在 $\boldsymbol{Q}$ 上的极小多项式为 $f(X)$，而 $f(X)$ 在 $\boldsymbol{C}$ 上分解为

$$f(X)=(X-\alpha_1)\cdots\cdots(X-\alpha_n),\ \alpha_i\in\boldsymbol{C},\alpha_1=\alpha.$$

因此可得 K 到 $\boldsymbol{C}$ 的 n 个嵌入

$$\sigma_j: K\longrightarrow\boldsymbol{C},$$
$$\alpha\longmapsto\alpha_j,\ (1\leqslant j\leqslant n).$$

注意 K 的每个元素 β 均是 α 的多项式 $\beta=h(\alpha)\in\boldsymbol{Q}[\alpha]$，$\sigma_j(\beta)=$

$\sigma_j(h(\alpha))=h(\alpha_j)\in C$. 于是令 $|\beta|_j=|\sigma_j(\beta)|_\infty$，即 $|h(\alpha)|_j=|h(\alpha_j)|_\infty$，就得到 K 的 n 个赋值 $|\ \ |_j(1\leqslant j\leqslant n)$. 但应注意 $|a+b\sqrt{-1}|=|a-b\sqrt{-1}|$，故若 $\alpha_j=\bar{\alpha}_k$ 则 $|\ \ |_j=|\ \ |_k$. 设 $\alpha_1,\cdots\cdots,\alpha_n$ 之中有 r_1 个实数，r_2 对共轭虚数，也就是说 K 到 C 有 r_1 个实嵌入(即嵌入到 R)，有 r_2 对共轭虚嵌入(即嵌入象不含于 R). 于是我们得到 K 的 $r=r_1+r_2$ 个赋值 $\infty_1,\cdots,\infty_r$，它们都是 Q 的 ∞ 的延拓，以后将证它们互不等价.

Q 的 p—adic 赋值的延拓也可类似如上得到，当然域 C 应代以有类似功能的域.

一般地，设 $(E,Q)\supset(F,P)$，P(从而 Q)是非阿基米德赋值. 则称 $f=f(Q|P)=[\bar{E}:\bar{F}]$ 为**剩余类次数**，其中 $\bar{E}$ 和 $\bar{F}$ 是 E 和 F 在 Q 和 P 的剩余类域；取指数赋值 $v\in Q$，则称

$$e=e(Q|P)=(v(E^*):v(F^*))$$

为 Q 在 P 的**分岐指数**，$v(E^*)=\{v(\alpha)|\alpha\in E^*\}$ 称为 E 的(加法)**赋值群**. P 到 E 的延拓个数记为 $g(P)$，或 $g_E(P)$.

系 1. 设 K 为 n 次数域，P 为其 $\wp$—adic 素除子，在 Q 上限制为 p 则

(1) $f(P|p)=f(\wp|p)$,

(2) $e(P|p)=e(\wp|p)$,

(3) $g(p)=g_K((p))$,

(4) $\sum\limits_{i=1}^{g(p)} e(P_i|p)f(P_i|p)=n$.

其中 $f(\wp|p)$，$e(\wp|p)$，及 $g_K((p))$ 分别为理想 $\wp$ 在 (p) 上的剩余类次数，分岐指数，及 (p) 在 K 的素理想因子个数，P_i 为 (p) 在 K 的素理想因子.

证明 (1) 由定理三证明已知 P 的赋值环为 $A_{\wp}$(A 在 $\wp$ 的局部化),赋值理想为 $\wp A_{\wp}$,故 $f(P|p)=[A_{\wp}/\wp A_{\wp}:\boldsymbol{Q}_p/p\boldsymbol{Q}_p]$,由第三章§1 定理知此即为 $[A/\wp:\mathbf{Z}/p\mathbf{Z}]=f(\wp|p)$.

(2) 取指数赋值 $v(\alpha)=\log_{p^{-1}}|\alpha|_{\wp}$. 于是由 $|p|_{\wp}=|p|_p=(\frac{1}{p})$ 知 $v(p)=1$;由 $|\pi|_{\wp}=(\frac{1}{p^{1/e}})$ 知 $v(\pi)=1/e$,其中 $\pi\in\wp-\wp^2$,$e=e(\wp|p)$. 故 $v(\boldsymbol{Q}^*)=\boldsymbol{Z}$, $v(K^*)=e^{-1}\mathbf{Z}$,即得(2).

(3) 由定理 2 即知.

(4) 由理想分解的相应等式即得. □

对于代数函数域 K 也有类似定理 3 的结果. 记 $k=F(X)$, K 为 k 的 n 次扩张. 则由定理 2 知 k 在 F 上平凡的素除子为 $\{\infty,p(X)\}$. K 的在 F 上平凡的素除子即为∞和诸 $p(X)$的延拓. 若素理想$(p(X))$在 K 中分解为 $\wp_1^{e_1}\cdots\cdots\wp_g^{e_g}$, 则$\wp_i$-adic 赋值为 $p(X)$的延拓,分岐指数为 e_i,剩余类次数为 $f_i=[\overline{K}_i:\overline{k}]$ $(1\leqslant i\leqslant g)$,其中 $\overline{K}_i=O_K/\wp_i$,$\overline{k}=F[X]/(p(X))$,O_K 是 $F[X]=O_k$ 在 K 上的整闭包. 特别当 $F=\boldsymbol{F}_q$ 为 q 元有限域时, $\overline{k}=\boldsymbol{F}_{q^d}$, $d=\deg p(X)$,故$\#\overline{K}_i=\#O_K/\wp_i=(\#\overline{k})^{f_i}=q^{f_id}$,这称为 $\wp_i$ 的绝对范数或次数. 当 K/k 为可分扩张时,由素分解的相应定理知 $\sum\limits_1^g e_if_i=n$; 但有时 K/k 可能是不可分的(这一点与数域情形不同).

习 题

1. 在定理 2 中设 $F=\boldsymbol{C}$ 为复数域,说明 $f\in\boldsymbol{C}(X)$的指数赋值与其极点和零点的关系.

§4.4 逼近定理

逼近定理揭示出不等价的有限个赋值是相互独立的. 这是孙子定理的推广,在处理多个赋值时将很重要.

定理 1 (逼近(Approximation)定理). 设 $\varphi_1,\cdots,\varphi_n$ 是域 K 的互不等价的非平凡赋值,记 $\varphi_i(x)=|x|_i$. 对 K 中任意元素 $b_1,\cdots,b_n$,任给 $\varepsilon>0$,必存在 K 中元素 x 使得

$$|x-b_i|_i<\varepsilon \quad (\text{对所有 } 1\leqslant i\leqslant n). \qquad \square$$

现若 $K=\boldsymbol{Q}$ 为有理数域,φ_i 是 p_i-adic 赋值,相应指数赋值记为 $v_{p_i}(i=1,\cdots,n)$. 对任意 $b_1,\cdots,b_n$,任取 $\varepsilon<(\frac{1}{p_i})^{m_i}$. 则由上述定理有 x 使 $|x-b_i|<\varepsilon<(1/p_i)^{m_i}$,这意味着 $v_{p_i}(x-b_i)>m_i$,即 $x-b_i\equiv 0(\bmod\ p_i^{m_i})$. 故逼近定理是孙子定理的推广. 下面可看到,二者的证明思路也类似.

引理 1 设 $\varphi_1,\cdots,\varphi_n$ 如定理 1,则存在 $x\in K$ 使 $|x|_1>1$, $|x|_2<1,\cdots\cdots,|x|_n<1$.

引理 2 设 $\varphi_1,\cdots,\varphi_n$ 如定理 1,任给 $\varepsilon>0$,存在 $y\in K$ 使 $|1-y|_1<\varepsilon,|y|_2<\varepsilon,\cdots,|y|_n<\varepsilon$.

引理 1 之证 对 n 归纳. 当 $n=2$ 时,由 §4.2 定理 2,存在 $b,c\in K$ 使 $|b|_1>1,|b|_2\leqslant 1,|c|_1\leqslant 1,|c|_2>1$(因为 T_2 不强于 T_1,T_1 也不强于 T_2);故取 $x=b/c$ 即可. 现设引理 1 对 $n-1$ 成

立，取 $b\in K$ 使 $|b|_1>1$，$|b|_i<1$ $(1\leqslant i\leqslant n-1)$；再取 $c\in K$ 使 $|c|_1>1$，$|c|_n<1$. 若 $|b|_n\leqslant 1$ 则取 $x=b^m c$ 即可(m 适当大). 现设 $|b|_n>1$. 对任一赋值 $\varphi(x)=|x|$，若 $|b|<1$ 则 $b^m\to 0$(对拓扑 T_φ)，从而 $\frac{b^m}{1+b^m}\to 0$，从而 $\left|\frac{b^m}{1+b^m}\right|\to 0$. 同样若 $|b|>1$ 则 $\frac{1}{b^m}\to 0$，从而 $\frac{b^m}{1+b^m}=\frac{1}{1+1/b^m}\to 1$，从而 $\left|\frac{b^m}{1+b^m}\right|\to 1$. 故取 $x=\frac{b^m c}{(1+b^m)}$ 即可(m 充分大).

引理 2 之证 取 x 如引理 1，令 $y=\frac{x^m}{1+x^m}$(m 待定). 则对 $i=2,\cdots\cdots,n$ 有 $|y|_i\to 0$，而

$$|1-y|_1=\left|\frac{1}{1+x^m}\right|_1=\left|\frac{1}{x^m}\right|_1\cdot\left|\frac{1}{1+1/x^m}\right|_1\to 0.$$

故 m 充分大时，y 满足引理 2.

定理 1 之证 取 $M=\max\{|b_j|_i\}$ $(i,j=1,\cdots\cdots,n)$. 由引理 2 知存在 $y_1,\cdots,y_n\in K$ 使

$$|1-y_i|_i<\varepsilon/M^n \quad (i=1,\cdots,n),$$

$$|y_j|_i<\varepsilon/M^n \quad (j\neq i).$$

故 $x=b_1y_1+b_2y_2+\cdots+b_ny_n$ 满足定理. □

§4.5 完备化

有理数域 $\boldsymbol{Q}$ 与实数域 $\boldsymbol{R}$ 的区别之一在于，$\boldsymbol{R}$ 中的柯西序列在 $\boldsymbol{R}$ 中都有极限，而 $\boldsymbol{Q}$ 则不然. 对于一般的域 K，设 v 是 K 的一赋值，序列 $\{a_n\}$ $(a_n\in K)$ 称为对于 v 的柯西(Cauchy)序列是指：对任意 m,n，当 $m,n\longrightarrow\infty$ 时，

$$a_m - a_n \longrightarrow 0 \quad (\text{对 } v \text{ 决定的拓扑 } T_v),$$

亦即

$$|a_m - a_n|_v \longrightarrow 0.$$

若 K 中对 v 的每个柯西序列在 K 中都有极限(即收敛于 K 中一元素),则称 K 对 v 是**完备的**(Complete),也称对 v 代表的素除子是完备的.例如 $\boldsymbol{R}$,$\boldsymbol{C}$ 对普通绝对值(无限赋值)是完备的,$\boldsymbol{Q}$ 则不然.正由于此,人们才引入了实数.

我们回忆从 $\boldsymbol{Q}$ 发展到 $\boldsymbol{R}$ 的途径,就是采用(承认)无限小数为新的数,也就是采用柯西序列为新的数,当然极限为 0 的柯西序列要等同于 0,从而极限相同(即相差一个极限为 0 的序列)的两个序列要相互等同.

对一般的有赋值 v 的域 K,我们也可按上述同样的方法构作新的完备域 K_v,满足:(1)K_v 是 K 的扩张,其赋值 v' 是 v 的延拓;(2)K_v 对 v' 是完备的;(3)K 在 K_v 中处处稠密.我们称(K_v,v')是 K 对 v 的**完备化**(Completion),也称(K_v,P')是 K 对 P 的完备化(其中 P 和 P' 是 v 和 v' 所在素除子).

有时,也将包含关系 $K \subset K_v$ 减弱为嵌入,而称满足如下条件的(K_v,v')是 K 对 v 的完备化:(1)有嵌入 $\sigma: K \longrightarrow K_v$,$|\sigma\alpha|_{v'} = |\alpha|_v$ 对 $\alpha \in K$ 成立;(2)K_v 对 v' 是完备的;(3)σK 在 K_v 处处稠密.

定理 1 设域 K 有赋值 v,则 K 对 v 的完备化 K_v 是存在的,且在 K-同构意义下是唯一的(即若(K_v,v')和(K_v',w)是 K 对 v 的两个完备化,则有 K-同构 $\sigma: K_v \to K_v'$ 使 $\sigma^* w = v'$).

证明 K 中元素构成的所有柯西序列形成一个环 R(加法和乘法定义为对应项相加、相乘),其中趋于 0 的序列全体 I 是

一个理想. 事实上,对于序列 $A=\{a_n\}\in R$,我们令

$$\phi(A)=|A|_{v'}=\lim_{n\to\infty}|a_n|_v,$$

则显然有(i) $|A|_{v'}\geqslant 0$,(ii) $|AB|_{v'}=|A|_{v'}|B|_{v'}$,(iii) $|A+B|_{v'}\leqslant |A|_{v'}+|B|_{v'}$. 由此易知 I 是 R 的理想. 作商环

$$K_v=R/I,$$

则 K_v 是一域. 事实上若 R 中 $A=\{a_n\}\notin I$,令

$$b_n=\begin{cases}0, & 若\ a_n=0,\\ \dfrac{1}{a_n}, & 若\ a_n\neq 0.\end{cases}$$

则显然$\{a_n\}\{b_n\}\equiv 1(\mathrm{mod}I)$.

上述 v' 可以认为定义在 K_v 上,这是由于对于 $N\in I$ 有

$$|A|_{v'}=|A+N-N|_{v'}\leqslant|A+N|_{v'}+|N|_{v'}=|A+N|_{v'}\leqslant|A|_{v'}.$$

于是由前述三性质知 v' 是 K_v 的赋值.

K 可看作是 K_v 的子域(每个 $a\in K$ 可看作是常数序列$\{a\}\in K_v$). 当然 K 在 K_v 中是处处稠密的,因为 K_v 的每个元素不外乎就是 K 中元素的极限(即序列).

最后证明 K_v 对 v' 是完备的,设$\{\alpha_n\}$是 K_v的柯西序列,由于 K 在 K_v 是稠密的,故对每个 n 存在着 $a_n\in K$ 使 $|\alpha_n-a_n|_{v'}<\frac{1}{n}$. 故$\{\alpha_n-a_n\}$是趋于 0 的序列,于是知$\{a_n\}$是柯西序列,以 $\alpha\in K_v$ 记$\{a_n\}$代表的(模 I)类,自然有 $v'(\alpha-a_n)\to 0$. 故 $v'(\alpha-a_n)\to 0$,即知$\{\alpha_n\}$收敛于 α,K_v 是完备的.

现设 K_v 和 $K_{v'}$ 是 K 的两个完备化,赋值分别为 v' 和 w. 对任一 $\alpha\in K_v$,则 $\alpha=\lim a_n$(对于 v'的拓扑),其中$\{a_n\}$是 K 上的 Cauchy 序列(因为 K 在 K_v 中处处稠密). 于是$\{a_n\}$也是 $K_{v'}$ 上的 Cauchy 序列,由于 $K_{v'}$ 是完备的,故其在 $K_{v'}$ 中有极限,记为 $\alpha'=\lim a_n$(对于 w 的拓扑). 故有映射

$$\sigma: K_v \to K_{v'}, \alpha \to \alpha'.$$

显然 σ 是域的同态，故是域的 K-嵌入. 由于 K_v 和 $K_{v'}$ 的对称性可知 σ 是域的同构，若视 σ 为等同，则下式说明 $v' = w$：

$$\begin{aligned} |\alpha|_{v'} &= |\lim a_n|_{v'} = \lim |a_n|_{v'} = \lim |a_n|_v \\ &= \lim |a_n|_w = |\alpha'|_w. \end{aligned}$$ □

系 1 设 L 是完备域(对赋值 w)，K 是其子域. 设 $\bar{K}$ 是 K 在 L 的闭包(对 w 决定的拓扑)，则 $\bar{K}$ 是 K 的完备化(对 w 在 K 的限制 v).

于是对 $\boldsymbol{Q}$ 的任一素数 p，我们有 p—adic 素除子 p，$\boldsymbol{Q}$ 对 p 的完备化记为 $\boldsymbol{Q}_p$. 因此我们有了无限多个完备域 $\boldsymbol{Q}_p$，它们的地位与 $\boldsymbol{R}$(是 $\boldsymbol{Q}$ 对∞的完备化)是相当的.

数域 K 对其各个(互相独立的)赋值 v 均有一完备化 K_v，也称为**局部域**. 相对来说，K 本身称为**整体域**，我们将看到，局部域的结构较简单，数学问题常较易处理. 对有一些理论，如果在每个局部域 K_v(包括无限赋值 v)均成立，则在整体域 K 中也就成立.(例如对二次型可解性，这称为 Hasse 原则). 但对有些问题不是这样. 虽然如此，这些问题在局部域上的研究还是能提供极有用的提示，因此是常常采用的途径.

系 2 设(K_v, v')是 K 对非阿基米德赋值 v 的完备化，v 和 v' 所在的素除子分别记为 P 和 P' 则

$$e(P'|P) = f(P'|P) = 1, \qquad \overline{K_v} = \overline{K}.$$

特别若 P 是离散的则 P' 也是. 而且 $O_{P'}$ 是 O_P 在 K_v 的闭包，$\wp_{P'}$ 是 $\wp_P$ 在 K_v 的闭包，这里 O_P 和 $\wp_P$ 表示 P 的赋值环和赋值理想.

证明 记$|x|=|x|_{v'}$. 因为K在K_v中处处稠密,故对任意$\alpha\neq 0\in K_v$,存在$a\in K$使$|a-\alpha|<|\alpha|$,从而$|\alpha|=|(a-\alpha)+\alpha|=|a|$. 这说明$e(P'|P)=1$. 而对任意$\alpha\in O_{P'}$, $|\alpha|=1$,存在$a\in K$使$|\alpha-a|<1$,故$|a|=1$(因$|\alpha|=1$),故$a\in O_P\subset O_{P'}$且$\alpha-a\in\wp_{P'}$,故$\bar{\alpha}=\bar{a}$, $f(P'|P)=1$.

设α属于O_P的闭包,则存在$a\in O_P$与α充分接近,则$|\alpha|=|a|\leqslant 1$,即$\alpha\in O_{P'}$. 若α不属于O_P的闭包,由于K在K_v稠密,故存在$a\in K-O_P$与α充分接近,从而$|\alpha|=|a|>1$, $\alpha\notin O_{P'}$. 同样证明$\wp_{P'}$是$\wp_P$的闭包. □

在具有非阿基米德赋值φ的域K中,极限问题(对于φ决定的拓扑)特别简单:

(i) 若$a_n\to a\neq 0$,则$\varphi(a_n)=\varphi(a)$对所有充分大的n成立.

(ii) $\{s_n\}$为 Cauchy 序列当且仅当$s_{n+1}-s_n\to 0$.

(iii) 若级数$\sum_1^\infty a_n$收敛于s,则任意重排级数各项顺序后仍如此.

(iv) 若$\sum a_n=s$, $\sum b_n=t$,则

$$\sum(a_n\pm b_n)=s\pm t,\qquad \sum_{k=1}^{\infty}\Big(\sum_{n+m=k}a_nb_m\Big)=st.$$

(v) 若K对φ是完备的,则$\sum a_n$收敛当且仅当$a_n\to 0$.

例如对于(i),当n充分大时$\varphi(a_n-a)<\varphi(a)$,于是$\varphi(a_n)=\varphi(a)$(否则$\varphi(a_n-a)=\max\{\varphi(a_n),\varphi(a)\}\geqslant\varphi(a)$). (ii)相当于说,$\sum a_n$是 Cauchy 级数当且仅当$a_n\to 0$,这由$|a_n+\cdots+a_m|\leqslant\max\{|a_n|,\cdots,|a_m|\}$即知. 其余由此易知.

定理 2(Ostrowski)　对于阿基米德素除子完备的域只有 $\boldsymbol{R}$ 和 $\boldsymbol{C}$ 两个(同构意义下),且其素除子即为 P_∞(即普通绝对值决定的无限素除子).

证明　设 K 对 P 完备,P 为阿基米德素除子,故 K 的特征必为 0,于是 $K\supset\boldsymbol{Q}$(同构意义下).P 在 $\boldsymbol{Q}$ 的限制必为∞,因为这是 $\boldsymbol{Q}$ 的唯一阿基米德素除子.于是 $\boldsymbol{Q}$ 对∞的完备化 $\boldsymbol{R}$ 含于 K,即为 $\boldsymbol{Q}$ 在 K 中的闭包.我们只需再证明 K 是 $\boldsymbol{R}$ 的代数扩张(注意若 K 为数域,这点无需再证),这样就可知 $K=\boldsymbol{R}$ 或 $\boldsymbol{C}$.至于 P,当 $K=\boldsymbol{R}$ 时显然 $P=P_\infty$(完备化唯一性,见定理 1).当 $K=\boldsymbol{C}$ 时,P 作为完备域 $\boldsymbol{R}$ 的素除子 P_∞ 的延拓是唯一确定的,只能是无限素除子,简证如下:取赋值 $\varphi\in P$ 使 φ 在 $\boldsymbol{R}$ 上限制为普通绝对值,对任意 $\alpha=a+b_i\neq 0\in\boldsymbol{C}$,由 $\varphi(i)=1$(因 $i^4=1$)可知

$$\begin{aligned}\varphi(\alpha)&\leqslant\varphi(a)+\varphi(b)=|a|+|b|\\&\leqslant\sqrt{2}\sqrt{|a|^2+|b|^2}=\sqrt{2}\,|\alpha|.\end{aligned}$$

令 $\psi(\alpha)=\varphi(\alpha)/|\alpha|\leqslant\sqrt{2}$,由 $\psi(\alpha)^n=\psi(\alpha)^n\leqslant\sqrt{2}$(对任意 $n>0$)知 $\psi(\alpha)\leqslant 1$.同理知 $\psi(1/\alpha)\leqslant 1$,故 $\psi(\alpha)=1$ ($\forall\,\alpha\neq 0$).即知 $\varphi(\alpha)=|\alpha|$.

现证 K 在 $\boldsymbol{R}$ 上是代数的(对数域 K,以下无需再证).任取 $t\in K$,$\alpha\in\boldsymbol{C}$,令 $f(\alpha)=\varphi(t^2-(\alpha+\bar{\alpha})t+\alpha\bar{\alpha})$,$\bar{\alpha}$ 为 α 的复共轭,显然 f 是 $\boldsymbol{C}$ 上实函数,是连续的:$|f(\alpha_1)-f(\alpha_2)|\leqslant\varphi((\alpha_1\overline{\alpha_1}-\alpha_2\overline{\alpha_2})+(\alpha_2+\overline{\alpha_2})t-(\alpha_1+\overline{\alpha_1})t)$.又易知当 $\alpha\to\infty$时 $f(\alpha)\to\infty$:

$$\begin{aligned}f(\alpha)&\geqslant\varphi(\alpha\bar{\alpha})-\varphi(t^2)-\varphi(\alpha+\bar{\alpha})\varphi(t)\\&\geqslant|\alpha|^2-\varphi(t^2)-2|\alpha|\varphi(t).\end{aligned}$$

令 $f(\alpha)$ $(\alpha\in\boldsymbol{C})$的最大下界为 m,显然 $m\geqslant 0$ 且存在 $\alpha\in\boldsymbol{C}$ 使 $f(\alpha)=m$(因为 $\alpha\to\infty$时,$f(\alpha)\to\infty$).记 $S=\{\alpha\in\boldsymbol{C}\,|\,f(\alpha)=m\}$,显然为非空有界闭集,故有 $\alpha_0\in S$ 使$|\alpha_0|\geqslant|\alpha|$($\forall\,\alpha\in S$).

若 $m=0$ 则 $f(\alpha_0)=0$，于是 t 满足 $\boldsymbol{R}$ 上二次方程. 再设 $m>0$，取 $0<\varepsilon<m$，令 $g(x)=x^2-(\alpha_0+\overline{\alpha_0})x+\alpha_0\overline{\alpha_0}+\varepsilon\in\boldsymbol{R}[x]$，设 $\alpha_1,\overline{\alpha_1}$ 为其二复根. 由 $\alpha_1\overline{\alpha_1}=\alpha_0\overline{\alpha}+\varepsilon$ 知 $|\alpha_1|>|\alpha_0|$，$\alpha_1\notin S$. 令

$$G(x)=(x^2-(\alpha_0+\overline{\alpha_0})x+\alpha_0\overline{\alpha_0})^n-(-\varepsilon)^n\in\boldsymbol{R}[x],$$

设其复根为 $\beta_1,\cdots\cdots,\beta_{2^n}$，且 $\beta_1=\alpha_1$. 于是

$$G(x)^2=\prod_1^{2n}(x^2-(\beta_i+\overline{\beta_i})x+\beta_i\overline{\beta_i}),$$

$$\varphi(G(t)^2)=\prod_1^{2n}f(\beta_i)\geqslant f(\alpha_1)m^{2n-1}.$$

而

$$\begin{aligned}\varphi(G(t))&\leqslant\varphi(t^2-(\alpha_0+\overline{\alpha_0})t+\alpha_0\overline{\alpha_0})^n+\varphi(-\varepsilon)^n\\&=f(\alpha_0)^n+\varepsilon^n=m^n+\varepsilon^n.\end{aligned}$$

此两不等式给出

$$f(\alpha_1)m^{2n-1}\leqslant\varphi(G(t))^2\leqslant(m^n+\varepsilon^n)^2,$$

$$f(\alpha_1)/m\leqslant(1+(\varepsilon/m)^n)^2.$$

令 $n\to\infty$，则得 $f(\alpha_1)/m\leqslant1$，$f(\alpha_1)=m$，$\alpha_1\in S$，矛盾. □

§4.6 离散赋值域

设域 F 有非阿基米德赋值 $\varphi: x\to|x|$. φ 对应着指数赋值 $v(x)=-\log|x|$（§4.2）. 域 F 的非 0 元的指数赋值全体 $v(F^*)$ 显然是 $\boldsymbol{R}$ 的加法子群，称为 v 的**赋值群**. 因此有两种情形：(1) $v(F^*)$ 是离散的，从而同构于 $\boldsymbol{Z}$（作为加法群）或为 0（当 φ 平凡时）；(2) $v(F^*)$ 在 $\boldsymbol{R}$ 中处处稠密. 这两种情形下分别称 v（和 φ 及其素除子）是**离散的**(**discrete**)或非离散的(nondiscrete). 例如数域 K 的 $\wp$-adic 赋值都是离散的.

现设域 F 有离散素除子 P，显然可取 P 中一个指数赋值 $v=v_P$ 使 $v(F^*)=\mathbf{Z}$，v 称为 P 的**标准指数赋值**，于是 F 中有元素 π 使

$$v(\pi)=1,$$

π 称为 F 对 v 的**素元素**或**局部一致化参数**. 例如对 $\boldsymbol{Q}$ 的 p－adic 素除子 p，$v(p^n)=n$，$\pi=p$.

先看 F 的理想. 显然 v 的赋值理想 $\wp=\pi O$，O 为赋值环. 而对任一正整数 r 有 O 的理想

$$\wp^r=\pi^r O=\{a\in F\mid v(a)\geqslant r\}.$$

当然 $\wp^r=aO$ 对满足 $v(a)=r$ 的任意 a 成立. 所以 $\wp$，$\wp^2$，$\wp^3$，…就是 O 的全部真理想. 故 $\wp$ 是 O 的唯一的素理想，也是唯一的极大理想，其余的真理想都是它的幂 $\wp^r=\pi^r O$. 因此 O 是主理想环，当然也就是 Dedekind 环. 故以前我们关于 Dedekind 环的分式域 K 的讨论对 F 都是适用的. 特别可知 O 是唯一析因环，而且它只有一个素元素(不计单位倍)，所以分解特别简单，每个 $a\in F$ 均可唯一分解为：

$$a=\pi^r u \qquad (r\in\mathbf{Z}, u \text{ 是 } O \text{ 的单位}).$$

显然 $O=\{\pi^r u\mid r\geqslant 0\}$，$\wp=\{\pi^r u\mid r\geqslant 1\}$. 显然理想 $\wp^r$ 的逆为分式理想

$$\wp^{-r}=\pi^{-r}O=\{a\in F\mid v(a)\geqslant -r\}.$$

于是我们有一个加法群的链：

$$F\supset\cdots\supset\wp^{-2}\supset\wp^{-1}\supset O\supset\wp\supset\wp^2\supset\cdots\supset\{O\} \tag{$*$}$$

因 $\wp^r=\{a\in F\mid v(a)>r-1\}$，故 $\wp^r$ 是中心在零的开集(从而也是闭的，因其补集是开的(是 $\wp^r$ 的(平移)陪集之并)). (如下考虑也可知 $\wp^r$ 是开的：对任一 $x\in F$，若 $y\in F$ 使 $|x-y|<|x|$，则 $|y|=|x|$). 故上述链($*$)构成 0 的一个基本开邻域系(称为一

串漏斗）. 显然我们有加法群的同构（对 $n>0, r\in\mathbf{Z}$）：

$$\wp^r\cong\wp^{r+n},$$

$$\wp^r/\wp^{r+n}\cong O/\wp^n,$$

$$\wp^r/\wp^{r+1}\cong O/\wp\cong\overline{F}.$$

同样，我们有乘法群链（漏斗）：

$$F^*\supset U\supset U_1\supset U_2\supset\cdots\cdots\supset\{1\}. \qquad (**)$$

其中

$$U_r=1+\wp^r \quad (r\geqslant 1),$$

为乘法群（若 $a=1+\pi^r u$ 则显然 $a\in U$，而由 $1=a^{-1}a=a^{-1}+\pi^r ua^{-1}$ 知 $a^{-1}=1-\pi^r ua^{-1}\in U_r$）. 于是由链（*）知道在拓扑群 F^* 中，链（**）构成 1 的基本开（且闭）的邻域系.

我们有群的同构（其中 R^+ 表示环 R 的加法群）：

(i) $F^*/U\cong\mathbf{Z}^+$ （事实上 $F^*\cong U\times\pi^{\mathbf{Z}}$）；

(ii) $U/U_1\cong\overline{F}^*$；

(iii) $U_r/U_{r+1}\cong\overline{F}^+\cong\wp^r/\wp^{r+1} \quad (r\geqslant 1)$.

事实上，(i)中的同构由指数赋值 $v: F^*\to\mathbf{Z}^+$ 决定，F^* 中元 $a=u\pi^n$. 对于(ii)考虑环同态的正合序列

$$\{0\}\to\wp\xrightarrow{i}O\xrightarrow{\psi}\overline{F}\to\{0\},$$

其中 i 为包含映射，ψ 是模 $\wp$ 剩余类映射. 考虑域 $\overline{F}$ 的乘法群 $\overline{F}^*$，$\psi^{-1}(\overline{F}^*)=U$，故我们有乘法群满同态 $\psi': U\to\overline{F}^*$，$a\longmapsto a+\wp$，其核为 $1+\wp=U_1$，故知(ii)，且有乘法群正合序列

$$\{1\}\to U_1\xrightarrow{i'}U\xrightarrow{\psi'}\overline{F}^*\to\{1\}.$$

为了证(iii)，注意 $a\longmapsto 1+\pi^r a$ 引起 1∶1 对应

$$O\leftrightarrow U_r=1+\pi^r O,$$

$$\wp\leftrightarrow U_{r+1}=1+\pi^{r+1}O.$$

复合映射 $f: U_r\to O\to\overline{F}^+$，$1+\pi^r a\longmapsto a\longmapsto\overline{a}$ 显然为群同态，

满射，核为U_{r+1}，即知$U_r/U_{r+1}\cong O/\wp\cong\overline{F}^+$.

4.6.1 离散赋值完备域 F

现设F对离散素除子P是完备的. 对每个非0剩余类$\alpha\in\overline{F}=O/\wp$，选取一个代表$\eta\alpha\in O$，对$0\in\overline{F}$令其代表为$\eta 0=0$. 记$R=\eta(\overline{F})$为$\overline{F}$的代表元全系. 例如当$F=\mathbf{Q}_p$时，常选$R=\{0,1,\cdots\cdots,p-1\}$.

定理1 设域F对离散素除子P完备，R为$\overline{F}$的一个完全代表元系，则F的每个非0元素b可唯一地表示为级数

$$b=\sum_{n=r}^{\infty}a_n\pi^n.$$

其中$a_n\in R$，π为F的素元，$r\in\mathbf{Z}$，$a_r\neq 0$ （$0\in K$表为$\sum_{-\infty}^{\infty}0\pi^n$）. 反之，每个这样的级数是$F$中一元素且$v(b)=r$.

证明 首先，定理中的级数部分和$S_m=\sum_{r}^{m}a_n\pi^n$显然是一个Cauchy序列（$|S_{m+t}-S_m|=|\sum_{m+1}^{m+t}a_n\pi^n|\leqslant|a_{m+1}\pi^{m-1}|\to 0$）. 因$F$是完备的故$\{S_n\}$收敛于$F$中某元素$b$（注意，如果$F$不是完备的，这样的级数在$F$中可能不收敛，故定理第二部分不成立）. 而由$a_r\neq 0$有$v(S_m)=r$，故$v(b)=r$（这也说明0只有唯一的表示$\sum_{-\infty}^{\infty}0\pi^n$，因为$v(0)=-\infty$）.

任取$b\neq 0\in F$，设$v(b)=r\neq-\infty$，则$b\pi^{-r}\in U$. 故$\overline{b\pi^{-r}}\neq 0$有代表元$a_r\neq 0\in R$，于是$v(b\pi^{-r}-a_r)>0$，$v(b-a_r\pi^r)>r$. 现设我们已找到$a_1,\cdots\cdots,a_m\in R$使$v(b-S_m)>m$，于是$(b-S_m)/\pi^{m+1}$

$\in O$ 与某 $a_{m+1}\in R$ 在同一剩余类，故 $v((b-S_m)/\pi^{m+1}-a_{m+1})>0$，$v(b-S_{m+1})>m+1$. 由归纳法可知，这样就得到了收敛于 b 的序列 $\{S_m\}$，即 $b=\sum_{r}^{\infty}a_n\pi^n$. 若还有 $b=\sum_{r'}^{\infty}a'_n\pi^n$，则 $r=v(b)=r'$，故 $0=\sum_{r}^{\infty}(a_n-a'_n)\pi^n$. 由前述 0 的表示的唯一性知 $a_n=a'_n(n\in\mathbf{Z})$，即知 b 的表示是唯一的. □

作为定理 1 的特别情形，设 $F=K_v$ 为数域 K 对 $\wp$-adic 赋值 v 的完备化. 设 $A=O_K$ 为 K 的整数环，$A_\wp=(A-\wp)^{-1}A$ 为 A 在 $\wp$ 的局部化（也即为 v 在 K 中的赋值理想，见 §4.3），$\wp'=\wp A_\wp$ 为 $A_\wp$ 的极大理想（也即为 v 在 K 的赋值素理想）. 再记 A_v 为 v 在 K_v 的赋值环，$\wp_v$ 为 v 在 K_v 的赋值理想，则三个环 $A\subset A_\wp\subset A_v$ 分别对其极大理想 $\wp,\wp',\wp_v$ 的商环是相等的：

$$A/\wp=A_\wp/\wp'=A_v/\wp_v.$$

事实上前一等号在第三章 §1 已知，后一等号在完备化讨论中已知（即 $f(P'|P)=1$ 或 $\overline{K}_v=\overline{K}$）.

因此 $\overline{K}_v=A_v/\wp_v$ 的代表元素 R 可取为 $A/\wp$ 的代表元素，故可取自整数环 A. 自然可以取素元 $\pi\in\wp-\wp^2$. 所以 K_v 的每个非 0 元可唯一表示为

$$b=\sum_{n=r}^{\infty}a_n\pi^n,\quad (a_n\in R\subset A,\quad \pi\in A).$$

例如 $\boldsymbol{Q}_p$ 中非 0 元素可表为：

$$\sum_{n=r}^{\infty}a_np^n,\qquad (a_n=0,1,\cdots,p-1).$$

这也说明 A_v 是 A 在 K_v 的闭包（$b\in A_v$ 当且仅当 $r\geqslant 0$，故 b 是 $\sum_{n=0}^{N}a_n\pi^n\in A$ 的极限（$N\to\infty$））. 同样知 $\wp_v$ 是 $\wp$ 在 K_v 的闭包

($b\in\wp_v$ 当且仅当 $r\geqslant 1$).

有时我们对 $\mathbf{Z}_p$ 中元素作如下简记:

$$(a_0,a_1,a_2,\cdots)=a_0+a_1p+a_2p^2+a_3p^3+\cdots.$$

循环部分加上画线,即$(\cdots,\overline{a_i,\cdots,a_{i+k}})=(\cdots a_i,\cdots,a_{i+k},a_i,\cdots,a_{i+k},\cdots)$.($k=1$ 时画线记为点).

例 1 当 $p=3$ 时我们有以下展式

$0=(0,0,\cdots)=(3,2,2,\cdots)$(注意后式不是标准表示).

$-1=2/(1-3)=2(1,1,\cdots\cdots)=(2,2,2\cdots\cdots)=(\dot{2})$,

$-5=0-5=(3,2,2,\cdots\cdots)-(2,1,0,\cdots)=(1,1,\dot{2})$,

$$\begin{aligned}\frac{1}{5}&=-16/(1-3^4)=-16(\overline{1,0,0,0})\\&=-(1,2,1)(\overline{1,0,0,0})=-(\overline{1,2,1,0})\\&=(3,\dot{2})-(\overline{1,2,1,0})=(2,\overline{0,1,2,1}).\end{aligned}$$

$\sqrt{7}=(1,1,1,0,2,\cdots\cdots)$,

$-\sqrt{7}=(2,1,1,2,0,\cdots\cdots)$.

一般地,对 $b\in\mathbf{Q}_p$ 易知 $b\in\mathbf{Q}$ 当且仅当 b 是"p 的循环级数".事实上,设 $b=\frac{r}{s}p^n\in\mathbf{Q}$,其中整数 r,s 与 p 互素.设 p 对模 s 的指数为 t,亦即

$$p^t\equiv 1 \pmod{s},$$

则

$$1-p^t=ms,(m\in\mathbf{Z}).$$

$$\frac{1}{s}=\frac{m}{1-p^t}=m(1+p^t+p^{2t}+\cdots\cdots)=m(\overline{1,0,\cdots\cdots,0}),$$

$$b=\frac{rp^n}{s}=rm(p^n+p^{n+t}+p^{n+2t}+\cdots\cdots)$$

$$=rm(0,\cdots,0,\overline{1,0,\cdots,0}).$$

由于 rm 是 p 的有限级数，故知 b 是 p 的循环级数. $-b=(p,p-1,p-1,\cdots\cdots)$，$-b$ 也是循环的. 反之易知 p 的循环级数必是有理数.

这样，我们得到：Q_p 即为如下形式的 p 的级数全体

$$b=\sum_{n=r}^{\infty}a_n p^n \qquad (r\in \mathbf{Z},\ a_n=0,1,\cdots,p-1).$$

注意 r 可以是负数. Q 即为其中全体循环级数. p-adic 整数环 $\mathbf{Z}_p$ 为满足 $r\geqslant 0$ 的级数全体. 局部(分式)环 $(\mathbf{Z}-(p))^{-1}\mathbf{Z}$（有时记为 $\mathbf{Z}_{(p)}$，即为 $\mathbf{Z}_p\cap Q$）即为 $r\geqslant 0$ 的循环级数全体. $\mathbf{Z}$ 即为 $r\geqslant 0$ 的有限级数全体.

例 2 设 $f(X,Y)=Y^2-(X^3+X)\in \mathbf{C}[X,Y]$，$f(X,Y)=0$ 是 $\mathbf{C}_2$ 中一曲线 V，称为椭圆曲线. 令

$$A=\mathbf{C}[X,Y]/(f(X,Y))=\mathbf{C}[x,y],$$

称为 V 的坐标环（显然为定义在 V 上的多项式函数全体，因为两多项式 $g,h\in \mathbf{C}[X,Y]$ 在 V 上取值相同当且仅当 $g\equiv h \pmod f$）. 其中 x,y 表示 X,Y 模 f 的同余类). 设

$$K=\mathbf{C}(x,y),$$

为 A 的分式环（显然为定义在 V 上的有理函数全体）. 对点 $P=(0,0)\in V$，

$$\wp=(x,y).$$

显然为 A 的极大理想，A 对 $\wp$ 的局部化称为在点 P 的局部化：

$$A_P=\left\{\frac{h(x,y)}{g(x,y)}\,\middle|\, g(0,0)\neq 0,\ g,h\in A\right\}$$

$$=\text{在 } P \text{ 点有意义的 } V \text{ 上有理函数全体}.$$

A_P 的极大理想

$$M_P=\wp A_P=(x,y)=(\frac{y^2}{1+x^2},y)=(y^2,y)=yA_P.$$

为主理想，$y=\pi$ 为 A_P 的素元. 故若 $b\in K$，则 $bA_P=M_P^n$，故 $b=uy^n$，u 为单位，$n\in\mathbf{Z}$. 所以 K 有离散指数赋值 $v=v_p$：

$$v(uy^n)=n.$$

记 K 对 v 的完备化为 K_v，A_v 为 A(或 A_P)在 K_v 的闭包(即 K_v 的赋值环)，$\wp_v$ 为 $\wp$ 在 K_v 的闭包，则 $A_v/\wp_v=A_P/M_P=A/\wp=\mathbf{C}$，

$$\begin{aligned}A_v&=\{a_0+a_1y+a_2y^2+\cdots\cdots|a_i\in\mathbf{C}\}\\&=\mathbf{C}[[y]]=\text{在 } P \text{ 点解析的函数全体},\end{aligned}$$

其中 $C[[y]]$ 表示 y 的幂级数全体.

由上述可以看出，只要曲线 V 在 P 点是光滑的(即极大理想 M_P 是主理想)，A_v 便是 $\mathbf{C}[[\pi]]$. 这说明，不同的曲线 V 和不同的点 P 有着同构的 A_v.(例如对于 $P=(0,0)$，V 为 $Y=X$ 或 $Y^2=X^3+X$ 或 $Y^7=X^{11}+X$ 时，均有同构的 $A_v=\mathbf{C}[[\pi]]$). A_v 的这一性质颇不同于 A，A_P 和 K.

习　题

1. 在 $\mathbf{Q}_2$ 中展开 ±5，±7，±12，$\pm1/5$，$\pm1/7$ 为幂级数.
2. 在 $\mathbf{Q}_3$ 中展开 ±2，±5，$\pm1/2$，$\pm1/5$.

§4.7　赋值的延拓(完备情形)

对于扩域 E/F，常需考查 F 的赋值在 E 中延拓的可能及个数. 当 F 为完备域时，将证明这种延拓是唯一存在的. 当 F 非完备时，可先将其完备化再作研究.

以下设域 F 对其素除子 P 是完备的，O 为赋值环，$\wp$ 为赋

值理想，E/F 为 n 次扩张. 如果 P 为阿基米德赋值，则 F 只能是 $\mathbf{R}$ 或 $\mathbf{C}$(Ostrowski 定理)，故 $E=\mathbf{R}$ 或 $\mathbf{C}$，P 的延拓是清楚的. 故以下设 P 是非阿基米德素除子. 我们要证明：

定理 1 设域 F 对非阿基米德素除子 P 是完备的，E 为 F 的 n 次扩张，则 P 到 E 有唯一的延拓 Q 且 E 对 Q 是完备的. 而且

(1) 任一 $\varphi\in P$ 到 E 的唯一延拓 $\varphi'\in Q$ 由下式决定：

$$\varphi'(\alpha)=\varphi(N(\alpha))^{\frac{1}{n}},\ (\alpha\in E).$$

其中 $N=N_{E/F}$ 为 E 到 F 的范映射；

(2) P 离散当且仅当 Q 离散；

(3) Q 的赋值环 O_Q 为 O_P 在 E 的整闭包；

(4) 若 $\sigma\alpha$ 与 α 为 F-共轭，则 $\varphi'(\alpha)=\varphi'(\sigma\alpha)$.

首先注意，如果 φ 到 E 的延拓 φ' 是唯一的，则 φ' 只能如定理中所定义. 事实上，若 $\alpha_2,\cdots,\alpha_n$ 是 $\alpha=\alpha_1$ 在 F 上的共轭元，则由延拓 φ' 的唯一性知 $\varphi'(\alpha_i)=\varphi'(\alpha)$(否则令 $\psi(\alpha)=\varphi'(\alpha_i)$则可得 φ 的另一延拓 ψ). 故知 $\varphi(N(\alpha))=\varphi'(\alpha_1\cdots\alpha_n)=\varphi'(\alpha_1)\cdots\cdots\varphi'(\alpha_n)=\varphi'(\alpha)^n$.

下述 Hensel 引理在赋值延拓及其它方面均十分重要. 它把 $f(X)\in O[X]$的分解与剩余类域上 $\bar{f}(X)\in\bar{F}[X]$的分解连系起来(其中对 $f(X)=\sum a_iX^i$，记 $\bar{f}(X)=\sum\bar{a}_iX^i$，$\bar{a}$ 表示 $a\in O$ 在 $\bar{F}=O/\wp$ 中的代表的类)：

Hensel 引理 设 F 对(非阿基米德)指数赋值 v 完备，多项式 $f(X)\in O[X]$. 若

$$\bar{f}(X)=G(X)H(X),$$

其中 $G(X),H(X)\in\bar{F}[X]$ 且互素，则存在 $g(X),h(X)\in O[X]$ 使

$$f(X)=g(X)h(X).$$

且 $\bar{g}(X)=G(X)$，$\bar{h}(X)=H(X)$，$\deg g(X)=\deg G(X)$（且若 $G(X)$ 或 $H(X)$ 是首一的，则相应地 $g(X)$ 或 $h(X)$ 是首一的）.

证明 不妨设 $G(X)$ 是首一的. 显然有 $g_1(X),h_1(X)\in O[X]$ 使 $\bar{g}_1=G$，$\bar{h}_1=H$；且 g_1 与 G，h_1 与 H 次数均相等，$g_1(X)$ 首一. 设

$$\bar{a}(X)G(X)+\bar{b}(X)H(X)=1\quad(a(X),b(X)\in O[X]).$$

于是 $f-g_1h_1$ 和 ag_1+bh_1-1 均属于 $\wp[X]$，记它们系数的指数赋值的最小值为 ε. 若 $\varepsilon=\infty$，即有 $f=g_1h_1$，则证毕. 再设 $0<\varepsilon<\infty$，设 $v(\pi)=\varepsilon(\pi\in F)$（当 v 离散时，无需求 ε，取 π 为素元即可），则显然 $f\equiv g_1h_1(\bmod\pi)$，$ag_1+bh_1\equiv 1(\bmod\pi)$.

我们将逐步构作一系列多项式 $g_n,h_n\in O[X]$ 满足(i) $f\equiv g_nh_n(\bmod\pi^n)$；(ii) $g_n\equiv g_{n-1}(\bmod\pi^{n-1})$，$h_n\equiv h_{n-1}(\bmod\pi^{n-1})$；(iii) $\bar{g}_n=G,\bar{h}_n=H$；(iv) $\deg g_n=\deg G=r$，$\deg h_n\leqslant\deg f-r=s-r$.

情形 $n=1$ 已完成. 设对 $n-1$ 已完成($n\geqslant 2$). 先设

$$g_n=g_{n-1}+\pi^{n-1}u(X),$$
$$h_n=h_{n-1}+\pi^{n-1}v(X).$$

其中 $u,v\in O[X]$ 待求. 若要 $f\equiv g_nh_n=g_{n-1}h_{n-1}+\pi^{n-1}(g_{n-1}v+h_{n-1}u)(\bmod\pi^n)$，只需 $w=(f-g_{n-1}h_{n-1})/\pi^{n-1}\equiv g_{n-1}v+h_{n-1}u$ $(\bmod\pi)$. 注意 $wag_1+wbh_1\equiv w(\bmod\pi)$，设 $wb=qg_1+u(X)$，其中 $\deg u(X)<\deg g_1(X)$，$u(X)\in O[X]$（因 g_1 首一）. 故 $(wa+qh_1)g_1+uh_1\equiv w(\bmod\pi)$. 将 $wa+qh_1$ 中同余于 $0(\bmod\pi)$ 的系数均换为零，得多项式 $v(X)$，则

$$vg_1+uh_1\equiv w(\bmod\pi),$$

即 $w=g_{n-1}v+h_{n-1}u \pmod{\pi}$，(i)得证. 只需再证(iv). 显然有 $\deg g_n=\deg g_{n-1}=r$(因 $\deg u<r$). 若 $\deg h_n>s-r$，则 $\deg v>s-r$，这与 $vg_1+uh_1\equiv w \pmod{\pi}$ 矛盾(因 $\deg g_1=r$，而 uh_1 和 w 的次数均 $\leqslant s$). 这就构造出了 g_n 和 h_n.

由于 F 完备，故序列 $\{g_n(X)\}$ 收敛于 $g(X)$，$\{h_n(X)\}$ 收敛于 $h(X)$ (事实上，记 $g_n(X)=\sum a_i^{(n)}X^i$，由 $g_{n+1}\equiv g_n \pmod{\pi^n}$ 知 $a_i^{(n+1)}\equiv a_i^{(n)} \pmod{\pi^n}$ 故 $\{a_i^{(n)}\}$ 是 Cauchy 序列，故 $a_i^{(n)}\to a_i\in O$). 故 $f\equiv g_nh_n\equiv gh \pmod{\pi^n}$ 对任一 n 成立，即知 $f=gh$. 其余显然. 证毕. □

系 1 设 F 对指数赋值 v 完备. (1) 若 $f(X)=a_nX^n+\cdots+a_1X+a_0\in F[X]$ 不可约，则

$$\bar{v}(f)\overset{\text{def}}{=\!=\!=}\min\{v(a_n),\cdots,v(a_0)\}=\min\{v(a_n),v(a_0)\}.$$

特别，若 f 是首一的，则 $f(X)\in O[X]\Leftrightarrow a_0\in O$.

(2) 若 $f(X)\in O[X]$ 首一且在 F 上不可约，则 $\bar{f}$ 在 $\bar{F}[X]$ 中为不可约多项式之幂.

(3) 若 $f(X)\in O[X]$ 且 $a_0\in\bar{F}$ 是 $\bar{f}(X)$ 的单根，则 $f(X)$ 有根 $\alpha\in O$ 使 $\bar{\alpha}=a_0$.

(4) $\boldsymbol{Q}_p$ 含 $p-1$ 次单位根群.

(5) 若 $p\equiv 1 \pmod 4$ 则 $\sqrt{-1}\in\boldsymbol{Q}_p$.

证 (1)适当乘以常数，不妨设 $f(X)\in O[X]$ 且 $\bar{v}(f)=0$. 若 $\min\{v(a_n),v(a_0)\}>0$，设 r 是使 $v(a_r)=0$ 的最大数. 由 $\bar{f}(X)=\bar{f}(X)\cdot 1=G(X)H(X)$ 及 Hensel 引理知，$f=g(X)h(X)$，$\deg g(X)=r>0$，$\deg h(X)=n-r>0$. 矛盾.

(2) 否则，由 Hensel 引理则给出 $f(X)$ 的一个分解.

(3) 于是 $\bar{f}=(X-a)H(X)$ 且 $(X-a)$ 与 H 互素. 由 Hensel 引理知 $f=gh$, $\deg g(X)=1$ 且首一,即 $g(X)=X-a\in O[X]$.

(4) $f(X)=X^{p-1}-1$ 在 $\boldsymbol{F}_p$ 中有单根 $\bar{1}$.

(5) X^2+1 在 $\boldsymbol{F}_p$ 中有单根.

定理 1 的证明 先证延拓的存在性,只需验证定理中的 ϕ 是 E 的赋值且在 F 上的限制为 φ. 后者显然. 又显然有 $\phi(\alpha)\geqslant 0$. $\phi(\alpha)=0\Leftrightarrow\alpha=0$. $\phi(\alpha\beta)=\phi(\alpha)\phi(\beta)$. 只需再证 $\phi(\alpha)\leqslant 1\Rightarrow \phi(1+\alpha)\leqslant 1$,便可知 ϕ 满足赋值定义中的 V3'. 设 $\alpha\in E$ 在 F 上的极小多项式为

$$f(X)=f(\alpha,F)=X^r+a_{r-1}X^{r-1}+\cdots+a_0\in F[X],$$

则 $N(\alpha)=\pm a_0^m$, $mr=n$. 故若 $\phi(\alpha)\leqslant 1$ 则 $\varphi(a_0)^m\leqslant 1$,故 $a_0\in O_P$. 由系 1(1)知 $f(X)\in O[X]$. 记 $g(X)=f(X-1)$ 为 $1+\alpha$ 的极小多项式,则

$$N(1+\alpha)=(\pm g(0))^m=(\pm f(-1))^m\in O_P,$$

故 $\phi(1+\alpha)\leqslant 1$.

由定义,显然 φ 离散当且仅当 ϕ 离散. 又显然 $O_P=O_Q\cap F$. 若 $\alpha\in O_Q$,则 $\phi(\alpha)\leqslant 1$,上述已证 $f(X)\in O_P[X]$,故知 α 在 O_P 上整. 反之,设 α 在 O_P 上整,则

$$\alpha^s+a_{s-1}\alpha^{s-1}+\cdots+a_0=0,\qquad a_i\in O_P.$$

$$\phi(\alpha)^s=\phi(a_{s-1}\alpha^{s-1}+\cdots+a_0)\leqslant\max_{0\leqslant i<s}\{\phi(\alpha)^i\},$$

故知 $\phi(\alpha)\leqslant 1$.

φ 延拓的唯一性和 E 的完备性来自于更一般的一个结果,即如下

定理 2 设 F 对赋值 φ 是完备域, V 是 F 上有限维线性空

间，则 V 上相容于 φ 的所有范数均是等价的（或称在等价意义下是唯一的），且 V 是完备的（对此范数的拓扑）.

设域 F 有赋值 φ，域 F 上线性空间 V 的相容于 φ 的一个**范数**（Norm，或称模）就是 V 上一个实值函数 ρ，且满足：(i) $\rho(x)\geqslant 0$；$\rho(x)=0\Leftrightarrow x=0$；(ii) $\rho(cx)=\varphi(c)\rho(x)$；(iii) $\rho(x+y)\leqslant\rho(x)+\rho(y)$（对任意 $x,y\in V,c\in F$）. 显然由距离 $d(x,y)=\rho(x-y)$ 决定 V 的一个拓扑. 两个范 ρ 与 ρ_2 称为**等价**是指存在正常数 c_1,c_2 使

$$c_1\rho(x)\leqslant\rho_2(x)\leqslant c_2\rho(x)$$

对任意 $x\in V$ 成立. 这也就是说，ρ 和 ρ_2 决定的度量拓扑是相同的. 例如 $\boldsymbol{C}$ 作为 $\boldsymbol{R}$ 上线性空间，$\rho(a+bi)=\sqrt{a^2+b^2}$ 定义一个范，因 $\boldsymbol{R}$ 对 ∞ 是完备的，此 ρ 在等价意义下是 $\boldsymbol{C}$ 的相容于 ∞ 的唯一范数.

由定理 2 可立得定理 1 的余下部分. 事实上，扩域 E 显然是 F 上的 n 维线性空间，E 的每一个赋值也为 E 的一个范，赋值等价相当于范等价. 故若 φ 到 E 上有两个延拓 φ_1 和 φ_2，则 φ_1 与 φ_2 等价，又因它们在 F 上的限制相等，故 $\varphi_1=\varphi_2$. □

定理 2 的证明 取定 V 的基 $w_1,\cdots\cdots,w_n$，任一 $x\in V$ 可表为 $x=a_1w_1+\cdots+a_nw_n$，$a_i\in F$. 令

$$\rho(x)=\max_i\{\varphi(a_i)\}.$$

则 ρ 是 V 上相容于 φ 的一个范数，显然 V 对 ρ 决定的拓扑是完备的. 只需再证任一相容于 φ 的范 ρ_2 与 ρ 是等价的. 取 $c_2=\rho_2(w_1)+\cdots\cdots+\rho_2(w_n)$，则显然有 $\rho_2(x)\leqslant c_2\rho(x)$. 其余部分对 n 归纳. $n=1$ 显然，设对 $n-1$ 情形结论成立. 令空间

$$V_i = Fw_1 \oplus \cdots \oplus Fw_{i-1} \oplus Fw_{i+1} \oplus \cdots \oplus Fw_n$$

由归纳假设知V_i对ρ_2的拓扑完备，从而在V中是闭的.故$V_i + w_i$闭.因$(V_1 + w_1) \cup \cdots\cdots \cup (V_n + w_n)$中不含0，故存在0的邻域与之无交，即存在$c_1 > 0$使

$$\rho_2(y_i + w_i) \geqslant c_1 \qquad (\forall\ y_i \in V_i, \forall\ i).$$

对任一$x = a_1 w_1 + \cdots\cdots + a_n w_n \neq 0$，设其第$j$个系数$a_j$的赋值最大：$\varphi(a_j) = \max\limits_i \{\varphi(a_i)\} = \rho(x)$，则

$$\rho_2(a_j^{-1} x) = \rho_2\left(\frac{a_1}{a_j} w_1 + \cdots + w_j + \cdots + \frac{a_n}{a_j} w_n\right) \geqslant c_1,$$

即知$\rho_2(x) \geqslant c_1 \varphi(a_j) = c_1 \rho(x)$. □

在定理1中，再设P是离散的，设v_P和v_Q分别是P和Q中标准指数赋值(即$v_P(F^*) = \mathbf{Z}$，$v_Q(E^*) = \mathbf{Z}$)，设$\pi = \pi_E$为E的素元，$e(Q|P) = (v_Q(E^*) : v_Q(F^*))$，$f = f(Q|P) = [\overline{E} : \overline{F}]$.

定理3 设如定理1，P是离散的，则

(i) $\pi_F = u\pi_E^e$（其中$u \in U_E$是E的单位)，且对任意$a \in F$有

$$v_Q(a) = e\ v_P(a).$$

(ii) $n = ef$，且$\{w_i \pi^j\}(1 \leqslant i \leqslant f, 0 \leqslant j \leqslant e-1)$为$E/F$的整基(即$O_Q$的$O_P$－基)，其中$w_i \in O_Q$使$\{\overline{w_i}\}$为$\overline{E}/\overline{F}$的基.

证明 (i)显然$v_Q(a) = \lambda v_p(a)$对某$\lambda \in \mathbf{R}$成立，以F的素元π_F代入知$v_Q(\pi_F) = \lambda v_P(\pi_F) = \lambda$，故$e = (v_Q(E^*) : v_Q(F^*)) = (\mathbf{Z} : \lambda \mathbf{Z}) = \lambda$.由此即知，若$u\pi_E^e \in F$，则为$F$的素元.

(ii)以$\mathfrak{Q} = (\pi)$和$\wp = (\pi_F)$表示Q和$\wp$的赋值理想，显然$\mathfrak{Q}$

是$\wp$在E上的唯一素理想因子，且$\wp O_Q=\mathfrak{D}^e$. 由扩域中素理想分解理论知$n=\sum_{i=1}^{g}e_if_i=ef$.

考虑

$$\alpha=a_1w_1+\cdots+a_fw_f, \qquad (a_i\in F)$$
$$\beta=b_0\pi^0+\cdots+b_{e-1}\pi^{e-1}. \qquad (b_j\in F)$$

我们断言：

(a) $v(\alpha)=\min\limits_i\{v(a_i)\}$,

(b) $v(\beta)=\min\limits_j\{v(b_j\pi^j)\}$.

事实上，不妨设a_j不全为0且$v(a_1)=\min\limits_i\{v(a_i)\}$. 则$a_i/a_1\in O_F$, $\alpha=a_1(w_1+(a_2/a_1)w_2+\cdots+(a_f/a_1)w_f)=a_1\alpha_1$, 由$\{\overline{w_i}\}$在$\overline{F}$上线性无关可知$\overline{\alpha}_1\neq\overline{0}$, 即知$v(\alpha_1)=0$, 故$v(\alpha)=v(a_1)$.

再看β, 如果$v(b_i\pi^i)=v(b_j\pi^j)$ $(i\neq j, b_i$与b_j非0), 则$v(\pi^{j-i})=v(b_j/b_i)\in v(F^*)$与$\pi$定义矛盾. 这就证明了上述断言.

由上述断言，易知$\{w_i\}$与$\{\pi^j\}$在F上线性无关. 现证$\{w_i\pi^j\}$线性无关. 为此只需证明

(c) $v(s_{ij})=v(\sum\limits_{i,j}c_{ij}w_i\pi^j)=\min\limits_{i,j}\{v(c_{ij}\pi^j)\}$.

为此先固定$0\leqslant j<e$, 若c_{ij}不全为0, 则

$$\begin{aligned}v(s_j)=v(\sum_i c_{ij}w_i\pi^j)&=v(\sum_i c_{ij}w_i)+v(\pi^j)\\&=\min_i\{v(c_{ij})\}+j\equiv j \pmod e.\end{aligned}$$

这是因为$v(c_{ij})$是$v(\pi_F)=v(\pi^e)=e$的倍数. 故对不同的j, $v(s_j)$是不同的，即得断言(c). □

习　题

1. 设域F对非阿基米德素除子P是完备的，Ω是F的任

一代数扩张. 则 P 到 Ω 有唯一延拓，且 O_Ω 是 $O_F=O_\Omega\cap F$ 在 Ω 中的整闭包，并有 $O_\Omega=\bigcup_E O_E$（E 过 Ω/F 的有限子扩张）.

2. 举例说明当 F 不是完备域时，Hensel 引理不成立.

3. 设如定理 3，则对任意 $\alpha\in E$，有 $v_P(N_{E/F}(\alpha))=fv_Q(\alpha)$.

§4.8 赋值的延拓（一般情形）

本节讨论一般的完全域 F 的赋值到其有限扩域 E 的延拓. 设域 F 有素除子 P，P 可为阿基米德的或非阿基米德的. 设 F_P 是 F 对 P 的完备化，Ω 为 F_P 的代数闭包（例如当 P 为阿基米德素除子时，$\Omega=C$）. P 到 F_P 有唯一的延拓，仍记为 P（或 $\tilde{P}$）. P 到 Ω 也有唯一的延拓（记为 P 或 P_Ω），这是由于对任一 $\alpha\in\Omega$，$F_P(\alpha)$ 是完备域 F_P 的有限扩张. 我们设所有的扩张都是可分的，例如我们最关心的数域情形即是如此，对不可分情形，也完全可以类似讨论.

例 1 设 $\boldsymbol{F}=\boldsymbol{Q}$，$P=\infty$，$F_P=\boldsymbol{R}$，$\Omega=\boldsymbol{C}$. 设 $E=\boldsymbol{Q}(w)$，w 在 $\boldsymbol{Q}$ 上的极小多项式为

$$f(X)=X^4+X^3+X^2+X+1\in\boldsymbol{Q}[X].$$

将 $f(X)$ 在 $\boldsymbol{R}[X]$ 中分解为不可约因子之积：

$$\begin{aligned}f(X)&=P_1(X)P_2(X)\\&=(X^2-X(\sqrt{5}-1)/2+1)(X^2+X(\sqrt{5}+1)/2+1)\\&=((X-w_1)(X-w_4))((X-w_2)(X-w_3))\end{aligned}$$

其中 $w=w_1=e^{2\pi i/5}$，$w_k=w_1{}^k$ $(1\leqslant k\leqslant 4)$. 于是

$$w_1=\overline{w}_4,\quad w_2=\overline{w}_3.$$

（其中 $\overline{w}$ 表示 w 的复共轭）. 注意 E 中元可表为 w 的多项式

$g(w), g(X)\in \boldsymbol{Q}[X]$，于是 E 到 $\boldsymbol{C}$ 有 4 个 $\boldsymbol{Q}$-嵌入

$$\mu_k:\quad E\longrightarrow \boldsymbol{C},$$
$$g(w)\longmapsto g(w_k).$$

由此定义∞到 E 的四个延拓：即对 $\alpha=g(w)\in E$，令

$$|g(w)|_{\infty_k}=|g(w_k)|.$$

但应注意，$\infty_1=\infty_4$，$\infty_2=\infty_3$. 这是因为 $w_1=\overline{w}_4$，$w_2=\overline{w}_3$ 故 $|g(w_1)|=|g(w_4)|$，$|g(w_2)|=|g(w_3)|$. 而$\infty_1\neq\infty_2$，事实上

$$|w|_{\infty_1}=|w|=|(\sqrt{5}-1)/4+i(\sqrt{10+2\sqrt{5}})/4|,$$

而 $$|w|_{\infty_2}=|w_2|=|(-\sqrt{5}-1)/4+i(\sqrt{10-2\sqrt{5}})/4|.$$

我们称 μ_1 与 μ_4 是在 $\boldsymbol{R}$ 上共轭的，这相当于说 w_1 与 w_4 是在 $\boldsymbol{R}$ 上共轭的. □

对每个素除子，我们取定其中一个赋值作为标准赋值. 因此素除子与标准赋值的讨论是对应的.

首先 F 的素除子 P 到扩域 E 中有一个明显的延拓方法，即将 E 嵌入到 Ω 中，由 P_Ω 诱导出 E 的素除子 Q，则 Q 为 P 的延拓. 详言之，因为 Ω 是含 F 的代数封闭域，E/F 是代数扩张，故共有 $n=[E:F]$个 E 到 Ω 的 F-嵌入：

$$\mu_i: E\longrightarrow\Omega\qquad (1\leqslant i\leqslant n).$$

P_Ω 到$(\mu_i E)F_P$ 的限制仍记为 P_Ω. 则 μ_i 将 P_Ω 传递（诱导）到 E 上为

$$Q_i=\mu_i^*(P_\Omega)=P_\Omega^{\mu_i},$$

则 Q_i 即为 P 到 E 的延拓（这里，对嵌入 $\mu: E\to\Omega$，$\mu^*(P)=P^\mu$ 定义如下：对 $\varphi\in P$，$\alpha\in E$，令

$$(\mu^*\varphi)\alpha=\varphi(\mu\alpha),$$

而 $\mu^*(P)=\{\mu^*\varphi|\varphi\in P\}$.（也记 $\mu^*P=P^\mu$，$\mu^*\varphi=\varphi^\mu$）.

定理1 设E/F为n次可分扩张，P为F的素除子，F_P为F对P的完备化，Ω为F_P的代数闭包.设

$$\mu_i : E \longrightarrow \Omega.$$

为E到Ω的n个F-嵌入.则

(1) P到E的全部延拓即为$Q_i=\mu_i^* P_\Omega \quad (1 \leqslant i \leqslant n)$；

(2) $Q_i=Q_j$当且仅当μ_i与μ_j在F_P上共轭，亦即$(\mu_i E)F_P$与$(\mu_j E)F_P$在F_P上共轭；

(3) E对Q_i的完备化$E_{Q_i}=(\mu_i E)F_P$.

证明 (1)已知每个嵌入μ_i确可诱导P到E的一个延拓$Q_i(1 \leqslant i \leqslant n)$.反之设$Q$是$P$到$E$的延拓，现证明$P$必由某$\mu_i$诱导.设$E$对$Q$的完备化为$\hat{E}$，$Q$到$\hat{E}$的延拓记为$\hat{Q}$.设$\hat{F}$为$F$在$\hat{E}$中的闭包，则$\hat{F}$是$F$的完备化.由完备化的唯一性可知$\hat{F}=F_P$(也就是说$\hat{F}$与$F_P$是$F$-同构的，我们将此$F$-同构视为等同). EF_P/F_P显然是有限扩张(因E/F为有限扩张)，故EF_P是完备的(因F_P完备)，从而EF_P是$\hat{E}$的闭子集.因为E在$\hat{E}$稠密，故EF_P在$\hat{E}$中稠密，即知

$$EF_P=\hat{E}.$$

于是知$\hat{E}/F_P$是有限扩张，故到F_P的代数闭包Ω有嵌入

$$\tau : \hat{E} \longrightarrow \Omega$$

(τ实为F—嵌入，因为我们将$\hat{F}$与F_P的F-同构视为等同).
记τ在E的限制为μ，则

$$\tau(\hat{E})=\tau(EF_P)=(\mu E)F_P.$$

同构τ将$\hat{E}$的素除子Q及其中赋值φ传递为$\tau(\hat{E})$的素除子$Q^{\tau^{-1}}$和赋值$\varphi^{\tau^{-1}}$(即对$\alpha \in \hat{E}$，$\varphi^{\tau^{-1}}(\tau\alpha)=\varphi(\alpha)$).但$\tau(\hat{E})$作为$\Omega$

的子域有素除子 P(即 P_Ω 的限制). 显然 $Q^{\tau^{-1}}$ 与 P 在 F 上限制相同(因为 Q 在 F 限制为 P,τ 在 F 上限制为 1). 由于 $\tau(\bar{E}\ )=(\mu E)F_P$ 的素除子是唯一的,故

$$Q^{\tau^{-1}}=P,$$

限制到 E 上即知 $Q=P^{\tau}=P^{\mu}=\mu^* P=Q_i$(某 $1\leqslant i\leqslant n$).

(2)若 μ_1 与 μ_2 是 F_P-共轭的,设 $\lambda:(\mu_1 E)F_P\cong(\mu_2 E)F_P$. 对 $\varphi\in P_\Omega,\alpha\in E$,知 $(\mu_2{}^*\varphi)\alpha=\varphi(\mu_2\alpha)=\varphi(\lambda\mu_1\alpha)=\varphi(\mu_1\alpha)=(\mu_1{}^*\varphi)\alpha$ (用到 $\varphi(\lambda\beta)=\varphi(\beta)$,因为 $\lambda\beta$ 与 β 在 F_P 上共轭). 即知 $Q_2=\mu_2{}^* P_\Omega=\mu_1{}^* P_\Omega=Q_1$.

反之,设 $Q_1=Q_2$,因为 μ_1 与 μ_2 是 F-嵌入,故有 F 上同构

$$\lambda:\mu_1 E\longrightarrow\mu_2 E,\qquad \mu_1 x\longmapsto\mu_2 x.$$

我们将可延长 λ 为 $(\mu_1 E)F_P$ 与 $(\mu_2 E)F_P$ 在 F_P 上的同构. 事实上,由于 $\mu_1 E$ 在 $(\mu_1 E)F_P$ 中稠密,故 $x\in(\mu_1 E)F_P$ 可写为

$$x=\lim_n\mu_1 x_n\qquad (x_n\in E)$$

序列 $\lambda\mu_1 x_n=\mu_2 x_n$ 也应收敛,这是因为 μ_1 与 μ_2 诱导出 E 的同一素除子,从而对任一 $\varphi\in P$ 有

$$\varphi(\mu_1 x_n)=(\mu_1{}^*\varphi)x_n=(\mu_2{}^*\varphi)x_n=\varphi(\mu_2 x_n).$$

记 $\lim\mu_2 x_n=\hat{\lambda}\ x$,则 $\hat{\lambda}\ x\in(\mu_2 E)F_P$(因 $(\mu_2 E)F_P$ 完备). 由此得到域同构

$$\hat{\lambda}\ :(\mu_1 E)F_P\xrightarrow{\cong}(\mu_2 E)F_P,$$

且显然 $\hat{\lambda}$ 保持 F_P 的元素不变.

(3) 由(1)的证明即知. □

系 1 设如定理 1,并设 $E=F(\alpha)$ 为 F 的 n 次可分扩张,α 在 F 上的极小多项式为 $f(X)$,且 $f(X)$ 在 F_P 的分解为

$$f(X)=p_1(X)\cdots p_r(X)\in F_P[X]$$

其中 $p_i(X)$在 F_P 上不可约. 则 F 的素除子 P 到 E 上恰有 r 个不同延拓 $Q_1,\cdots,Q_r$. 若设 $p_i(X)$的次数为 n_i,在 Ω 中根为 $\alpha_{ij}(1\leqslant j\leqslant n_i)$,则

$$\mu_{ij}:\alpha \longmapsto \alpha_{ij}.$$

$(1\leqslant i\leqslant r,1\leqslant j\leqslant n_i)$恰为 E 到 Ω 的 n 个 F-嵌入,μ_{ij}与 $\mu_{i'j'}$在 F_P 上共轭当且仅当 $i=i'$(即 α_{ij}与 $\alpha_{i'j'}$在 F_P 上共轭). 而

$$Q_i=\mu_{ij}^*(P), \qquad (i=1,\cdots,r).$$

(对任一个 $1\leqslant j\leqslant n_i$).

系 2 设如定理 1,若 Q 为 P 的延拓则记为 $Q|P$ 或 $Q\supset P$. 设 E_Q 为 E 对 Q 的完备化(称为**局部域**),记

$$n_Q=[E_Q:F_P],$$

称为**局部扩张次数**,设 N_Q 和 Tr_Q 分别为 E_Q 到 F_P 的范和迹映射. 设 $f(\alpha,E/F)=f(\alpha,F)^{[E:F(\alpha)]}$为 α 在 E/F 中的域多项式,其中$f(\alpha,F)$为 α 在 F 上的不可约多项式,α 为 E 中任意元素,则

(1) $n=\sum\limits_{Q|P}n_Q$ (整体扩张次数是局部次数之和).

(2) $N_{E/F}(\alpha)=\prod\limits_{Q|P}N_Q(\alpha)$ (整体范是局部范之积).

(3) $T_{rE/F}(\alpha)=\sum\limits_{Q|P}Tr_Q(\alpha)$ (整体迹是局部迹之和).

(4) $f(\alpha,E/F)=\prod\limits_{Q|P}f(\alpha,E_Q/F_P)$ (整体域多项式是局部域多项式之积).

若 P 为 F 的阿基米德素除子,则 $F_P=\boldsymbol{R}$ 或 $\boldsymbol{C}$(Ostrowski 定理),依次称 P 为实的或**复的素除子**.

系 3 设 P 为 F 的阿基米德素除子,E/F 为 n 次扩张. 则

(1) 若 P 为复的，则 P 到 E 有 n 个延拓 Q_i，且均是复的.

(2) 若 P 为实的，则 P 到 E 有 r_1 个实延拓 $Q_1,\cdots,Q_{r_1}$，有 r_2 个复延拓 $Q_{r_1+1},\cdots,Q_{r_1+r_2}$，其中 r_1 和 $2r_2$ 是 E 到 C 的 F-实嵌入(即 E 的象属于 $\boldsymbol{R}$)和 F-复嵌入的个数，$r_1+2r_2=n$. 且 $n_{Q_i}=2$ 或 1(依 Q_i 为实或复).

证明 设 $E=F(\alpha)$，α 在 F 上的极小多项式为 $f(X)$. 若 P 为复的，则 $F_P=\mathbf{C}$，$f(X)$ 在 F_P 上分解为一次因子之积. 若 P 为实的，则 $F_P=\boldsymbol{R}$，$f(X)$ 在 $\boldsymbol{R}$ 上分解为二次和一次不可约因子之积. 再由定理 1 或系 1 即得证. □

系 4 设 $K/\boldsymbol{Q}$ 是 n 次数域，$v_0\in M_{\boldsymbol{Q}}$ 是 $\boldsymbol{Q}$ 的一个素除子，$\alpha\in K$. 对于 v_0 到 K 的延拓 v，记 $n_v=[K_v:\boldsymbol{Q}_{v_0}]$ 为局部次数. 则

$$\prod_{v|v_0}|\alpha|_v^{n_v}=|N_{K/\boldsymbol{Q}}(\alpha)|_{v_0}.$$

证明 K 到 Ω(=$\boldsymbol{Q}_{v_0}$的代数闭包)的嵌入共 n 个：$\mu_1,\cdots\cdots,\mu_n$. 每个 μ_i 给出 v_0 的延拓 v_i：$|\alpha|_{v_i}=|\mu_i\alpha|_{v_0}$(这里 v_0 是指它到 Ω 的唯一延拓). 由 $N(\alpha)=\mu_1(\alpha)\cdots\mu_n(\alpha)$ 知

$$\begin{aligned}|N(\alpha)|_{v_0}&=|\mu_1(\alpha)|_{v_0}\cdots\cdots|\mu_n(\alpha)|_{v_0}=\prod_{i=1}^{r}|\alpha|_{v_i}^{n_{v_i}}\\&=\prod_{v|v_0}|\alpha|_v^{n_v}.\end{aligned}$$

□

如果 F 的素除子 P 到 n 次扩域 E 上有 n 个不同的延拓 $Q_1,\cdots\cdots,Q_n$，则称 P 在 E **完全分裂**. 由系 2(1)知，这相当于 $n_{Q_i}=1$ $(1\leqslant i\leqslant n)$，也即

$$E_{Q_i}=(\mu_i E)F_P=F_P.$$

对于固定的 i，常可将 E 与 $\mu_i E$ 等同. 于是我们有

系 5 F 的素除子 P 在 E 完全分裂当且仅当对其任一延拓 Q 有 $E_Q=EF_P=F_P$，即 $E\subset F_P$.

特别当 E/F 为数域的 n 次扩张时，F 的非阿基米德素除子 P 对应于素理想 $\wp$，其延拓 Q 对应于 $\wp$ 在 E 的素理想因子 $\mathfrak{P}$，若记 $\wp$ 在 E 的分裂域为 E^d，则 E^d 的完备化

$$E_Q^d=F_P,$$
$$E\cap F_P=E^d.$$

后者是因为 E^d 是 $\wp$ 在其中完全分裂的 E 的最大子域，也是含于 F_P 的 E 的最大子域.

例 2 由于奇素数 p 在 $E=\boldsymbol{Q}(\zeta_{p-1})$ 完全分裂，故 $\boldsymbol{Q}(\zeta_{p-1})\subset\boldsymbol{Q}_p$. 这说明 $\boldsymbol{Q}_p$ 含 $p-1$ 次单次根.

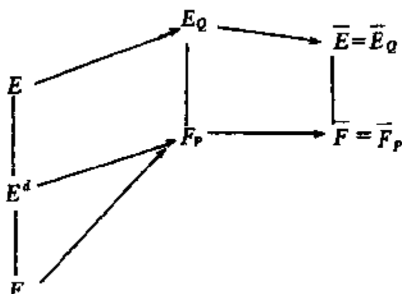
现设 E/F 为 n 次 Galois 扩张，$\mathrm{Gal}(E/F)=G$. 设 F 的素理想 $\wp$ 在 E 有素理想因子 $\mathfrak{P}$，$G_{\mathfrak{P}}$ 为 $\mathfrak{P}$ 的分解群. 以 P 和 Q 记 $\wp$ 和 $\mathfrak{P}$ 决定的素除子，记 F_P 和 E_Q 为相应的完备化.

系 6 设 E/F 为 Galois 扩张，则 E_Q/F_P 也是 Galois 扩张，且有自然同构：

$$G(E_Q/F_P)\cong G_{\mathfrak{P}}=\mathrm{Gal}(E/E^d).$$

证明 由于 $E_Q\supset E$，故有限制映射

$$\varphi: G(E_Q/F_P)\longrightarrow G(E/F).$$



对任一$\lambda\in G(E_Q/F_P)$，因为在完备域F_P上共轭的元素α和$\lambda\alpha$有相同的赋值，故λ不改变E_Q的赋值理想$\wp_Q=\{\alpha\,|\,|\alpha|<1\}$，故$\varphi(\lambda)$不改变$\mathfrak{P}=\wp_Q\cap E$，亦即$\varphi(\lambda)\in G_{\mathfrak{P}}$. 反之，对任一$\lambda_0\in G_{\mathfrak{P}}\subset G$，由连续性可将$\lambda_0$延长为$\lambda\in G(E_Q/F_P)$（事实上，$\alpha\in E_Q$是$E$上级数$\sum a_n$，令$\lambda(\sum a_n)=\sum(\lambda_0 a_n)$即可）. 这说明$\varphi$的象为$G_{\mathfrak{P}}$. 又$\varphi$显然是单射（若$\lambda_0=1$则$\lambda=1$）. 即得引理. □

在系6情形下，设E_Q的赋值环和赋值理想为B_Q，$\wp_Q$. 对B_Q（也称对E_Q）作模$\wp_Q$剩余映射：$E_Q\longrightarrow\overline{E}_Q=B_Q/\wp_Q$. 此映射限制到$E,E^d,F_P,F$上依次相当于作模$\mathfrak{P}=\wp_Q\cap E$，$\wp_d=\wp_Q\cap E^d$，$\wp_P=\wp_Q\cap F_P$，$\wp=\mathfrak{P}\cap F$的剩余映射. 从而得到$\overline{E}_Q=\overline{E}$，$\overline{F}_P=\overline{E^d}=\overline{F}$. 于是$f(\wp_Q|\wp_P)=[\overline{E}_Q:\overline{F}_P]=[\overline{E}:\overline{F}]=f(\mathfrak{P}|\wp)$.

习　题

1. (1)说明数域扩张L/K中的素分解与K的$\wp$—adic赋值到L上延拓的关系. 二者间e,f,g的关系.

(2) 说明L/K与完备化L_w/K_v及剩余类域$\overline{L}/\overline{K}$间的关系，分解域与惯性域如何？

2. (1)分别求$\boldsymbol{Q}$到$\boldsymbol{Q}(i)$，$\boldsymbol{Q}(\sqrt{2})$，$\boldsymbol{Q}(\sqrt{-3})$的所有赋值延

拓($i=\sqrt{-1}$).

(2) 求 $\boldsymbol{Q}$ 的无限赋值∞到 $\boldsymbol{Q}(\sqrt[3]{2})$的所有延拓.

3. 设 $f(X)=X^3-2$,α 是其一根,$K=\boldsymbol{Q}(\alpha)$. 设 $\boldsymbol{Q}$ 的素除子 P 到 K 的延拓为 $Q_1,\cdots,Q_g$. 试对下列 P 求局部次数 $n_i=n_{Q_i}$,$e_i=e(Q_i|P)$,$f_i=f(Q_i|P)$:$P=\infty$,5,7,11,13,17,19,23,29,31.

第五章　局部域及应用

设 K 为数域，或者是常数域为有限域的代数函数域(即 $F_q(X)$ 的有限扩张). 常称 K 为**整体域**. 设 M_K 为 K 的素除子集，对其中每个素除子 P 取定一个标准赋值 v，作完备化 K_v，K_v 称为**局部域**. 为了研究 K 及 K 上的代数对象，常常要先对每个 v 研究 K_v 及 K_v 上的对象.

因此本章中常设域 F 对离散素除子 P 是完备的，v 是 P 中标准指数赋值(即 $v(F^*)=\mathbf{Z}$)，相应的绝对值(赋值)记为 $\varphi=|\quad|_v=|\quad|$. 取定 F 的素元 π，$v(\pi)=1$. 固定 F 的一个代数闭包 Ω，并设 F 的任意代数扩张 $E\subset\Omega$. 记 P，v，φ 到 E 的唯一延拓为 Q，v，φ，记 E 的标准指数赋值为 v_E，故 $v(a)=ev_E(a)$. 记 O_E，$\wp_E=\mathfrak{B}$，U_E 为 E 的赋值环，素理想和单位群，记 $O=O_F$，$\wp=\wp_F$，$U=U_F$. 记 $e=e(Q|P)=e(E/F)=e(\mathfrak{B}|\wp)=(v_E(E^*):v_E(F^*))$，$f=f(Q|P)=f(E/F)=f(\mathfrak{B}|\wp)=[\overline{E}:\overline{F}]$，$\overline{E}=O_E/\mathfrak{B}$，$\overline{F}=O/\wp$. 我们已知 $ef=[E:F]=n$. 对 $\alpha\in O_E$，记 $\overline{\alpha}\in\overline{E}$ 为 α 所在的模 $\mathfrak{B}$ 剩余类.

§5.1　局部域上多项式

关于完备域上的多项式，我们已知有著名的 Hensel 引理

(§4.7)，本节继续讨论.

引理 1 设正整数 $m\not\equiv 0 \pmod{\wp}$，$x\in\wp$，则 $(1+x)^{1/m}\in U$.

证 考虑 $(1+x)^{1/m}$ 展开的二项式级数，系数的分母均不属于 $\wp$，故此级数收敛. □

定理 1（**Newton 求根法**） 设 $f(X)\in O[X]$，$a_0\in O$ 满足

$$|f(a_0)/f'(a_0)^2|=r<1, \qquad r\neq 0,$$

则可在 a_0 附近求得 $f(X)$ 一根 $\alpha\in O$. 详言之，令

$$a_{i+1}=a_i-f(a_i)/f'(a_i), \qquad (i=0,1,\cdots)$$

则 $\{a_i\}$ 收敛于 $f(X)$ 一根 $\alpha\in O$，且

$$|\alpha-a_0|\leqslant|f(a_0)/f'(a_0)|\leqslant r<1.$$

证 先归纳证明以下三结论：

(i) $|a_i|\leqslant 1$，

(ii) $|a_{i+1}-a_i|=|f(a_i)/f'(a_i)|\leqslant|f(a_i)/f'(a_i)^2|\leqslant r^{2^i}$，

(iii) $|a_i-a_0|\leqslant|f(a_0)/f'(a_0)|\leqslant r$

也将得出

$$|f'(a_{i+1})|=|f'(a_i)|.$$

首先注意 $a_0\in O$，$f(a_0)\in O$，$f'(a_0)\in O$，$|f'(a_0)|\leqslant 1$，$|f(a_0)|\leqslant r$，$|f(a_0)/f'(a_0)|\leqslant r<1$，故 $i=0$ 时上述结论成立. 设对 i 结论成立，于是由 Taylor 展开及 a_i 和 $f(a_i)/f'(a_i)$ 均属于 O 可知

$$\begin{aligned}|f(a_{i+1})|&=|f(a_i-f(a_i)/f'(a_i))|\\&=\left|f(a_i)-f'(a_i)\frac{f(a_i)}{f'(a_i)}+(O\text{ 中元})\left(\frac{f(a_i)}{f'(a_i)}\right)^2\right|\end{aligned}$$

$$\leqslant |f(a_i)/f'(a_i)|^2.$$

$$f'(a_{i+1}) = f'(a_i - f(a_i)/f'(a_i))$$
$$= f'(a_i) + (O\ \text{中元})(f(a_i)/f'(a_i)).$$

由(ii) 知$|f'(a_{i+1})/f'(a_i)| = 1$. 于是

$$\left|\frac{f(a_{i+1})}{f'(a_{i+1})^2}\right| \leqslant \frac{f(a_i)/f'(a_i)^{\ 2}}{|f'(a_i)|^2} = \left|\frac{f(a_i)}{f'(a_i)^2}\right|^2 \leqslant r^{2^{i+1}},$$

即得(ii). 上式也说明$|f(a_{i+1})/f'(a_{i+1})^2| \leqslant |f(a_i)/f'(a_i)^2|$,故$|f(a_{i+1})/f'(a_{i+1})| \leqslant |f(a_i)/f'(a_i)|$. 这就得出(iii). 值得注意的是,每个 a_i 均可作为牛顿法的出发点(即 a_0). 现由(ii),$\{a_i\}$是 Cauchy 序列. 再由(i) 知 a_i 趋于 $\alpha \in O$. 由$|f(a_i)| \leqslant r^{2^i}$知$|f(a_i)|$趋于$|f(\alpha)|$. 由(iii)知$|\alpha - a_0| \leqslant |f(a_0)/f'(a_0)|$. □

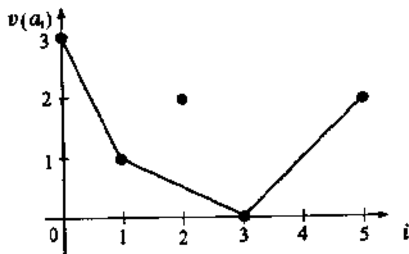
Newton **折线法**是另一有趣的方法,可用以得到关于多项式的因子及根的大小的信息. 设

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X], \qquad a_0a_n \neq 0.$$

在实平面 $\boldsymbol{R}^2$ 中取点集

$$S_f = \{(i, v(a_i)) \mid a_i \neq 0, 0 \leqslant i \leqslant n\},$$

并设 S_f 的下凸边界为折线 N_f,称为牛顿折线. (也就是说,N_f 是由 S_f 中一些点连成的下凸折线,使得 S_f 的其余点位于 N_f 之上).



例如对 $f(X)=-8-2X-4X^2+X^3-4X^5\in\mathbf{Q}_2[X]$，

$$S_f=\{(0,3),(1,1),(2,2),(3,0),(5,2)\}$$

故 $N_f=((0,3),(1,1),(3,0),(5,2))$.

定理 2 设 $((r,v(a_r)),(s,v(a_s))$ 是 $f(X)$ 的牛顿折线 N_f 的一边(即相邻点)，$r<s$，记此边斜率为 $-m=(v(a_s)-v(a_r))/(s-r)$. 则 $f(X)$ 恰有 $s-r$ 个根 $\alpha_1,\cdots,\alpha_{s-r}\in\Omega$ 的指数赋值为 m：

$$v(\alpha_1)=\cdots=v(\alpha_{s-r})=m,$$

且 $f_m(X)=(X-\alpha_1)\cdots(X-\alpha_{s-r})\in F[X]$ 是 $f(X)$ 在 F 上的一个因子.

证 不妨设 $a_n=1$. 设 $\alpha_1,\cdots,\alpha_n\in\Omega$ 为 $f(X)$ 的根，并设 $v(\alpha_1)=\cdots=v(\alpha_{s_1})=m_1$，$\cdots$，$v(\alpha_{s_t+1})=\cdots=v(\alpha_n)=m_{t+1}$，且 $m_1<m_2<\cdots<m_{t+1}$. 于是易知

$$v(a_n)=v(1)=0,$$
$$v(a_{n-1})=v(\alpha_1+\cdots+\alpha_n)\geqslant\min\{v(\alpha_i)\}=m_1,$$
$$v(a_{n-2})=v(\alpha_1\alpha_2+\cdots+\alpha_{n-1}\alpha_n)\geqslant\min\{v(\alpha_i\alpha_j)\}=2m_1,$$
$$\cdots\cdots$$
$$v(a_{n-s_1})=\min\{v(\alpha_{i_1}\cdots\alpha_{i_{s_1}})\}=s_1m_1,$$
$$v(a_{n-s_1-1})\geqslant s_1m_1+m_2,$$
$$\cdots\cdots$$

故 S_f 右边一些点为 $(n,0),(n-1,m_1),(n-2,2m_1),\cdots$ 在一条直线上，故显然 Newton 折线 N_f 的顶点为(从右向左)：

$$(n,0),(n-s_1,s_1m_1),(n-s_2,s_1m_1+(s_2-s_1)m_2),\cdots$$

而折线边的斜率依次(从右向左)为：

$$-m_1,-m_2,-m_3,\cdots\cdots.$$

只需再证 $f_m(X)\in F[X]$. 对 n 做归纳法. 设对 $<n$ 的情形

成立. 设 α_1 的极小多项式为 $P_1(X)\in F[X]$,则 $P_1(X)$的根的赋值都相等(从而为 $v(\alpha_1)=m_1$),故 $P_1(X)\mid f_{m_1}(X)$. 因

$$\left(\frac{f_{m_1}}{P_1}\right)(f_{m_2}\cdots f_{m_{t+1}})=\frac{f(X)}{P_1(X)}\in F[X]$$

的次数$<n$,由归纳法假设知左边的两个因子均属于 $F[X]$,即知 $f_{m_1}(X)\in F[X]$. 同理可得 $f_{m_i}(X)\in F[X]$. □

例 1 $f(X)=-8-2X-X^2+X^3\in \boldsymbol{Q}_2[X]$. 易知 $f(X)$无有理根. $S_f=\{(0,3),(1,1),(2,0),(3,0)\}$. 在 $\boldsymbol{R}^2$ 中画出 S_f 则显然 Newton 折线为 $N_f=S_f$. 三个边的斜率分别为$-2,-1,0$,故 $f(X)$有三根 $\alpha_1,\alpha_2,\alpha_3\in \boldsymbol{Q}_2$ 满足 $v(\alpha_1)=2$, $v(\alpha_2)=1$, $v(\alpha_3)=0$.

再用牛顿求根法,试取 $a_0=0$,则 $v(f(0))=3$, $2v(f'(0))=2$,满足定理 1. 故 a_0 可被加工为 $f(X)$的一个根 a 且 $v(a)=v(a-a_0)\geqslant v(f(0)/f'(0))=2$,即知 $a=\alpha_1$. 顺次可算得 $a_0=0$, $a_1=-4$, $a_2=-68/27$,等等. 注意在计算过程中可以取新的起点 a'_0,以使计算简单. 由于 $\alpha_i\notin \boldsymbol{Q}$,我们不能指望在 $\boldsymbol{Q}$ 中得到确值. 可以得出 $\alpha_1,\alpha_2,\alpha_3$ 的近似值 20,22,87 等.

系 1 设 $u=a_0+a_1p+a_2p^2+\cdots$为 $\boldsymbol{Q}_p$ 的单位($a_i\in \boldsymbol{Z}$),则 u 是 $\boldsymbol{Q}_p$ 中平方元当且仅当

$$\begin{cases}a_0\ \text{是二次剩余}(\bmod p), & \text{当 } p\neq 2;\\ u=1+a_3 2^3+\cdots, & \text{当 } p=2.\end{cases}$$

证明 设 $p\neq 2$. 若 $u=\varepsilon^2\in U^2$,则 $a_0=\bar{u}=\bar{\varepsilon}^2$ 是二次剩余. 反之,若 a_0 是二次剩余,设 $X^2-\bar{u}=(X-\bar{b})(X+\bar{b})$. 由 Hensel 引

理知 $X^2-u=(X-a)(X+a)$，$u=a^2\in\mathbf{Q}_p^{*2}$.

再设 $p=2$. $\varepsilon\in\mathbf{Q}_p$ 是单位意味着 $\varepsilon=1+a_1 2+\cdots$，故 $\varepsilon^2\equiv1\pmod{8}$. 反之若 $u\equiv1\pmod{8}$，考虑 $f(X)=X^2-u$，则 $v(f(1))\geqslant3>2=2v(f'(1))$. 故由 Newton 求根法知 1 可被加工为 $f(X)$ 在 $\mathbf{Q}_2$ 中一根，故 $u\in\mathbf{Q}_2^{*2}$. □

引理 2(**Krasner 引理**). 设 $\alpha,\beta\in\Omega$(F 的代数闭包)且 α 在 F 上可分，设

$$|\beta-\alpha|<|\sigma\alpha-\alpha|\qquad(\forall\ \sigma\neq1)$$

对所有 $F(\alpha)/F$ 的同构 $\sigma(\neq1)$ 成立，则 $\alpha\in F(\beta)$.

证明 只须证对 $F(\beta,\alpha)/F(\beta)$ 的任一同构 τ，有 $\tau\alpha=\alpha$. 由 $\tau\beta=\beta$ 及完备域赋值开拓的唯一性可知

$$|\beta-\tau\alpha|=|\tau\beta-\tau\alpha|=|\beta-\alpha|<|\sigma\alpha-\alpha|,$$

故

$$|\tau\alpha-\alpha|=|(\tau\alpha-\beta)+(\beta-\alpha)|\leqslant|\beta-\tau\alpha|<|\sigma\alpha-\alpha|$$

对所有 $F(\alpha)$ 的同构 $\sigma\neq1$ 成立，这意味着 τ 在 $F(\alpha)$ 的限制为 1，故 $\tau\alpha=\alpha$，$\alpha\in F(\beta)$. □

Krasner 引理说明，当 α,β 靠得充分近时，它们就代数相关. 我们可以用此研究多项式的根. 设 $f(X),g(X)\in F[X]$ 次数均为 n，均首 1. 设 $f(X)$ 有(r_i 重)根 $\alpha_i\in\Omega(1\leqslant i\leqslant d)$. 以 $|f(X)|$ 表示 $f(X)$ 系数绝对值的极大值. 易知若 $|f(X)|$ 有界则 $f(X)$ 的根的绝对值也有界. 现若 $g(X)$ 充分靠近 $f(X)$，即 $|f-g|$ 很小，对 g 的根 β，则

$$|f(\beta)-g(\beta)|=|f(\beta)|$$

也很小，故 β 靠近 f 的某根 α. 当 β 很靠近 α 时，β 与 $\alpha_i(\neq\alpha)$ 的

距离近乎$|\alpha-\alpha_i|$，故有下界；此时称β**属于**α. 当g充分靠近f时，对f的r重根α，必有g的r个根$\beta_1,\cdots,\beta_r$属于α. 否则就有一系列的多项式$\{g_k\}$逼近f，每个g_k有$s(\neq r)$个根$\beta_1^{(k)},\cdots,\beta_s^{(k)}$属于$\alpha$. 于是知$\lim g_k=f$，$\alpha$为$s$重根，矛盾.

定理 3 若$f(X)$不可约，可分，$g(X)$充分靠近$f(X)$，则$g(X)$也不可约. 对$f(X)$的任一根α，必存在$g(X)$的根β属于α，且$F(\alpha)=F(\beta)$.（这里仍设f,g均为n次首1多项式）.

证 因$f(X)$的根均为单根，f与g充分靠近，故g的根也均为单根，分别靠近$f(X)$的根. 由 Krasner 引理可知$\beta\in F(\alpha)$，$\alpha\in F(\beta)$. 即得$F(\alpha)=F(\beta)$. 由此即知$g(X)$不可约. □

系 2 对p-adic 数完备域$\boldsymbol{Q}_p$的任一n次扩张M，必存在$\boldsymbol{Q}$的n次扩张K使得K在M中稠密，且$K\boldsymbol{Q}_p=M$为K的完备化.

证 设$M=\boldsymbol{Q}_p(\alpha)$，$f(X)$为$\alpha$在$\boldsymbol{Q}_p$上的极小多项式. 取$g(X)\in\boldsymbol{Q}[X]$充分靠近$f(X)$，设$g(X)$的根$\beta$属于$\alpha$，令$K=\boldsymbol{Q}(\beta)$. 由$\boldsymbol{Q}_p(\beta)=\boldsymbol{Q}_p(\alpha)=M$即知$K\boldsymbol{Q}_p=M$. □

因此在研究完备域$\boldsymbol{Q}_p$的扩域时，可以设这些扩域是整体域的完备化，从而易于讨论.

习　题

1. 在$\boldsymbol{Q}_3$中求$\sqrt{-2}$.
2. 用 Newton 折线法证明 Eisenstein 多项式不可约.

§5.2 非分歧扩张

设 E/F 为 n 次扩张如本章开始所设. 若 $e=1$, 即 $f=n$, 亦即

$$[E:F]=[\overline{E}:\overline{F}],$$

并且 $\overline{E}/\overline{F}$ 是可分的, 则称 E/F (或 $\wp_E$ 对 $\wp$) 为**非分歧的** (unramified). 这是一类特别重要的扩张. 对 $f(X)=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_0$. 记 $\overline{f}(X)=\overline{a}_nX^n+\overline{a}_{n-1}X^{n-1}+\cdots+\overline{a}_0$.

引理 1 设 r 是 $\overline{F}$ 上的代数元, 则存在 F 上的代数元 α 使得 $\overline{\alpha}=r$ 且满足如下条件 (记 $E=F(\alpha)$):

(i) $\overline{F(\alpha)}=\overline{F}(\overline{\alpha})$;

(ii) $[E:F]=f(E/F)$, $e(E/F)=1$;

(iii) 若 $f(X)$ 是 α 在 F 上的极小多项式, 则 $\overline{f}(X)$ 是 $\overline{\alpha}$ 在 $\overline{F}$ 上的极小多项式.

证明 设 $[\overline{F}(r):\overline{F}]=n$, 则 r 在 $\overline{F}$ 上的极小多项式 $G(X)\in\overline{F}[X]$ 次数为 n, 并可设 $G(X)=\overline{F}(X)$, $f(X)\in F[X]$ 为 n 次. 设

$$f(X)=(X-\alpha_1)\cdots(X-\alpha_n),\quad \alpha_i\in O_\Omega$$

则

$$\overline{f}(X)=(X-\overline{\alpha}_1)\cdots(X-\overline{\alpha}_n)$$

不妨设 $r=\overline{\alpha}_1$, 并记 $\alpha_1=\alpha$, 记 $E=F(\alpha)$, 则

$$\begin{aligned} n &=[\overline{F}(\overline{\alpha}):\overline{F}]\leqslant[\overline{F(\alpha)}:\overline{F}]=f(E/F)\\ &\leqslant e(E/F)f(E/F)=[E:F]\leqslant n. \end{aligned}$$

从而均为等号, 且 $[E:F]=n$ 也说明 $f(X)$ 不可约. □

定理 1　E/F 非分歧$\Leftrightarrow E=F(\alpha)$，其中 α 是首一多项式 $f(X)\in O[X]$的根，且 $\bar{\alpha}$ 是 $\bar{f}(X)$的单根．而且在这种情形下，

(i) $\bar{E}=\bar{F}(\bar{\alpha})$；

(ii) $\{1,\alpha,\cdots,\alpha^{n-1}\}$是 E/F 的整基(即 O_E 的 O—基)．

证　($\Rightarrow$)：因为 $\bar{E}/\bar{F}$ 是可分的，故为单扩张，即存在 $r\in\bar{E}$ 使 $\bar{E}=\bar{F}(r)$．应用引理 1，知存在 $\alpha=\alpha_1\in\Omega$ 使 $r=\bar{\alpha}$，$F(\alpha)$在 F 上是非分歧的且$[F(\alpha):F]=[E:F]=n$．只需再证明 $\alpha\in E$．注意存在 $\beta\in O_E$ 使 $\bar{\beta}=r=\bar{\alpha}$，这意味着$|\beta-\alpha|<1$．因 $\bar{\alpha}$ 在 $\bar{F}$ 上可分，故引理 1 中 $\bar{\alpha}_i\neq\bar{\alpha}_j$，$\overline{\alpha_i-\alpha_j}\neq 0$ ($i\neq j$ 时)．由于 $\alpha_i-\alpha_j\in O_\Omega$，故$|\alpha_i-\alpha_j|=1$．即知$|\beta-\alpha|<|\alpha_i-\alpha|(i\neq 1)$．由上节 Krasner 引理可知 $\alpha\in F(\beta)\subset E$．

注意$\{1,\bar{\alpha},\cdots,\bar{\alpha}^{n-1}\}$是 $\bar{E}$ 的 $\bar{F}$—基，$e=1$．故由前章§7 定理 3 (ii)知$\{1,\alpha,\cdots,\alpha^{n-1}\}$是 E/F 的整基．

($\Leftarrow$)：由条件知，若 $g(X)$是 α 的首一多项式则 $\bar{\alpha}$ 是 $\bar{g}(X)$ 的单根．故从开始即可假设$f(X)$是 α 的极小多项式．由前章§7. Hensed 引理的系知，$\bar{f}(X)$只能是不可约多项式的幂，但 $\bar{\alpha}$ 是 $\bar{f}(X)$的单根，故 $\bar{f}(X)$不可约．故 $\deg f(X)=\deg\bar{f}(X)$，$n=[F(\alpha):F]=[\bar{F}(\bar{\alpha}):\bar{F}]\leqslant[\bar{E}:\bar{F}]=f\leqslant n$，故知 $f=n$，E/F 非分歧．

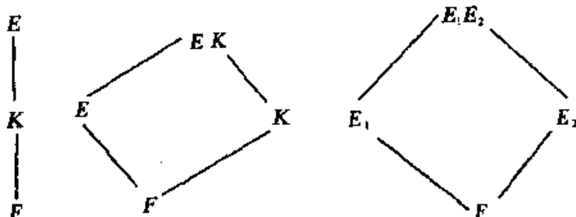
由证明过程易知，非分歧扩张 E/F 一定是可分的．这是由于 $\alpha_i\neq\alpha_j$ (当 $i\neq j$ 时)．　□

系 1　非分歧性满足如下性质(设 E/F 是有限扩张)：

(i)(传递性)若 $E\supset K\supset F$，则 E/F 非分歧当且仅当 E/K 和 K/F 均非分歧；

(ii)（提升性）若 E/F 非分歧，K/F 是任一有限扩张，则 EK/K 非分歧；

(iii)（复合性）若 E_1/F，E_2/F 均非分歧，则 E_1E_2/F 非分歧.



证 (i) 由剩余类域次数和域扩张次数的链性；

(ii) 由定理 1，若 $E=F(\alpha)$则 $EK=F(\alpha)$；

(iii) 由(i)和(ii).

系 2 设 E_1/F，E/F 均为有限扩张，E_1/F 非分歧，则 $\overline{E}_1\subset\overline{E}\Leftrightarrow E_1\subset E$.

证 这包含在定理 1 的证明中．由于 $E_1=F(\alpha)$，$\bar{\alpha}\in\overline{E}_1\subset\overline{E}$，设 $\beta\in O_E$ 使 $\bar{\alpha}=\bar{\beta}$，则由定理 1 证明知 $\alpha\in F(\beta)\subset E$.

系 3 每个有限扩张 E/F 均有一个最大非分歧子扩张 E'/F，且 E' 包含 E 的所有非分歧的子域．(E' 称为 E 的**惯性子域**).

证 考虑 $\overline{E}/\overline{F}$，设其最大可分子扩张为 $\overline{E}_1/\overline{F}$，则为单扩张，由定理 1 知 $\overline{E}_1=\overline{F(\alpha)}=\overline{F}(\bar{\alpha})$，$E_1=F(\alpha)$在 F 上非分歧．故 $E_1\subset E$（系 2）．如果 E'/F 是 E 的非分歧子域，则 $\overline{E'}\subset\overline{E}$. 由 $\overline{E'}/\overline{F}$ 可分知 $\overline{E'}\subset\overline{E_1}$，再由系 2 即知 $E'\subset E_1$. □

定理 2　F 的非分歧扩张集$\{E/F\}$到 $\overline{F}$ 的可分扩张集$\{\overline{E}/\overline{F}\}$有格同构 μ：　$E\to\overline{E}$.

证　(格同构意味着保持交及复合). 系 1 说明非分歧扩张集确实形成一个格(半序集且任二非分歧扩张的交及复合仍是非分歧的),显然 μ 是满射(定理 1,$\overline{E}=\overline{F(\alpha)}=\overline{F}(\bar{\alpha})$). 系 2 说明 μ 是单射,系 2 也说明 μ 及其逆均是保序的,从而 μ 保持交及复合:$\overline{E_1E_2}=\overline{E}_1\overline{E}_2$,$\overline{E_1\cap E_2}=\overline{E}_1\cap\overline{E}_2$. □

以下定理对 F 为数域的完备化,或 F 为有限域上有理函数域的完备化适用.

定理 3　设 $\overline{F}$ 为 q 元有限域 $q=p^r$,p 为素数,则

(i) F 的有限非分歧扩张集与 $\overline{F}$ 的有限扩张集之间格同构,且 F 的有限非分歧扩张 E/F 均为循环扩张;

(ii) 对任一固定的正整数 f,f 次非分歧扩张 E/F 存在且唯一,即 $E=F(\zeta)$,ζ 是任意 q^f-1 次本原单位根.

(iii) 设 $\zeta\in\Omega$ 是 m 次本原单位根,$(m,p)=1$,则 $E=F(\zeta)$ 是 F 的非分歧扩张. 而且 $f=f(E/F)$是满足

$$q^f\equiv 1\pmod{m}$$

的最小正整数,且$\{1,\zeta,\cdots,\zeta^{f-1}\}$是 E/F 的整基.

证　因 $\overline{F}$ 是完全域,故(i) 由定理 2 即得. Gal $(\overline{E}/\overline{F})$为循环群,生成元为 $\sigma:\bar{\alpha}\longmapsto\bar{\alpha}^q$ $(\forall\ \bar{\alpha}\in\overline{E})$. 于是由定理 1 的证明知 E/F 为 Galois 扩张,由 Galois 扩张素分解的理论知 Gal $(E/F)\cong$Gad $(\overline{E}/\overline{F})$,故为循环群.

(ii) $\overline{F}$ 的 f 次扩张唯一,故由(i) 知 E 唯一. 由定理 1 知 E 非分歧.

(iii) 因 F 的特征为 0 或 p,故有 m 次本原单位根 $\zeta\in\Omega$,满足 $f=X^m-1$. 故 $\overline{f}$ 与 $\overline{f}'=mX^{m-1}$互素,$\overline{f}$ 只有单根,由定理 1 知$F(\zeta)$是 F 的非分歧扩张. 注意由两方程

$$f(X)=X^m-1=\prod_{i=0}^{m-1}(X-\zeta^i),$$

$$\overline{f}(X)=X^m-1=\prod_{i=0}^{m-1}(X-\overline{\zeta}^i)$$

及引理 1 知 $1,\overline{\zeta},\cdots,\overline{\zeta}^{m-1}$恰为 $\overline{\Omega}$ 中 m 个 m 次单位根,故 $\overline{\zeta}$ 为本原单位根. 注意 Galois 群 $\overline{G}=\mathrm{Gal}\,(\overline{E}/\overline{F})$是 $f=[\overline{E}:\overline{F}]$阶循环群,生成元为

$$\sigma:\overline{\zeta}\longmapsto\overline{\zeta}^q.$$

故 f 是使 $\sigma^f=1$ 的最小正整数,而 $\sigma^f=1$ 相当于 $\overline{\zeta}^{q^f}=\overline{\zeta}$,即

$$\overline{\zeta}^{q^f-1}=1.$$

恰相当于 $q^f-1\equiv0\ (\mathrm{mod}\ m)$(因为 $\overline{\zeta}$ 是 m 次本原单位根). □

§5.3 完全分歧扩张

对 n 次扩张 E/F,若 $e=n$, $f=1$,则称 E/F 为**完全分歧扩张(或纯分歧扩张)**. 此时 $\overline{E}=\overline{F}$. 首先回忆

$$f(X)=X^n+a_1X^{n-1}+\cdots+a_n,\qquad a_i\in O_F\qquad(*)$$

称为 Eisenstein 多项式是指$v(a_n)=1$, $v(a_i)\geqslant1$. $(i=1,2,\cdots,n-1)$.

定理 1 (i)设 E/F 为完全分歧扩张,π 为 E 的一素元,则 π 在 F 上的极小多项式 $f(X)$为 Eisenstein 多项式且 $E=F(\pi)$.

(ii) 设$f(X)\in F[X]$是 Eisenstein 多项式，$\pi\in\Omega$ 是其一根，则 $E=F(\pi)$是 F 的完全分歧扩张，π 是 E 的素元，$f(X)$不可约.

证 设π的极小多项式为$f(X)$如$(*)$式，$a_i\in F$. 因π是在O_F上的整元素，故 $a_i\in F$. 自然知 $n\leqslant[E:F]=e$. 由

$$\pi^n+a_1\pi^{n-1}+\cdots+a_{n-1}\pi+a_n=0, \qquad (**)$$

可知左侧中至少有两项取得最低指数赋值．由$v(a)=v_E(a)=ev_F(a)$知左侧各项指数赋值依次为

$$\{n,\ ev_F(a_1)+(n-1),\ \cdots,\ ev_F(a_{n-1})+1,\ ev_F(a_n)\}$$

因模e剩余依次为$n,n-1,\cdots,1,0$. 且$e\geqslant n\geqslant 2$，故知$(**)$式左侧只能首尾两项达最小值，即

$$ev_F(a_i)+(n-i)>n=ev_f(a_n).$$

特别知 $e\leqslant n$，说明 $n=e=[E:F]$，$E=F(\pi)$. 由此也知道 $v_F(a_n)=1$，$v_F(a_i)\geqslant 1\ (i=1,2,\cdots,n-1)$. (i) 得证．

(ii)写$f(X)$如$(*)$式，代入π得$(**)$式，注意π是代数整数，故$v(\pi)=v_E(\pi)\geqslant 0$. 此时$(**)$式左侧的$v$值依次为

$$\{nv(\pi),\ ev_F(a_1)+(n-1)v(\pi),\ \cdots,\ ev_F(a_{n-1})+v(\pi),\ e\}.$$

除第一项外，其余各项中 e 最小，因不能只有一个最小项，故知 $nv(\pi)\fallingdotseq 0$ 且 $n\,v(\pi)=e\leqslant[E:F]\leqslant n$，即得$v(\pi)=1$，$e=n$，$f(X)$不可约． □

在定理 1 的情形可知$\{1,\pi,\cdots,\pi^{n-1}\}$是 E/F 的整基(参见上章 § 7 定理 3(ii)).

定理 2 设 E/F 为 n 次扩张且 $\bar{E}/\bar{F}$ 可分，则存在中间域 $F\subset E_1\subset E$ 使 E_1/F 为非分歧扩张，E/E_1 为完全分歧扩张；且有

单位 $\beta\in U_E$ 使$\{1,\beta,\cdots,\beta^{n-1}\}$为 E/F 的整基.

证 设 E_1 为 E/F 的最大非分歧扩张,因为 $\overline{E}/\overline{F}$ 可分,故而 $\overline{E}_1=\overline{E}$,这说明 E/E_1 是完全分歧的. 由上节知道,存在 $\alpha\in U_E$ 使 $E_1=F(\alpha)$,$\overline{E}=\overline{E}_1=\overline{F}(\bar\alpha)$,$f(X)$为 α 的极小多项式,$\bar f(X)$ 为 $\bar\alpha$ 的极小多项式,$\bar\alpha$ 是 $\bar f(X)$的单根(这相当于说 $v(f'(\alpha)=0)$,且$\{1,\alpha,\cdots,\alpha^{f(E_1/F)-1}\}$是 E_1/F 的整基,现取 E 的素元 π,令

$$\beta=\alpha+\pi,$$

显然$v(\beta)=0$,$\beta\in U_E$. 由于 $\bar\beta=\bar\alpha$ 及$f(E_1/F)=f(E/F)=f$,故 $1,\bar\beta,\cdots,\bar\beta^{f-1}$是 $\overline{E}/\overline{F}$ 的基. 由$f(\alpha)=0$,$v(f'(\alpha)=0$,及 Taylor 展开

$$f(\beta)=f(\alpha+\pi)=f(\alpha)+\pi f'(\alpha)+\pi^2\,(O_E\text{ 中元}).$$

知$v(f(\beta))=v(\pi)=1$. 故由上一章 §7 定理 3 的证明知 $\{\beta^i f(\beta)^j\}$是 E/F 的整基($0\leqslant i\leqslant f-1,0\leqslant j\leqslant e-1$). 故

$$O_E=\sum_{i,j}O_F\beta^i f(\beta)^j\subset O_F[\beta]\subset O_F+O_F\beta+\cdots+O_F\beta^{n-1}\subset O_E$$

即知$\{1,\beta,\cdots,\beta^{n-1}\}$是 E/F 的整基.

§5.4 顺分歧扩张

本节设 F 的特征为 p. 考虑有限扩张 E/F. 如果 $p\nmid e=e(E/F)$且 $\overline{E}/\overline{F}$ 可分,则称 E/F 为**顺分歧**(或**弱分歧**)的(tamely ramified). 若 $p\mid e$ 则称 E/F 为**野分歧**(或**强分歧**)的(wildly ramified). 当 $p=0$ 时,也称是顺分歧的.

我们已经看到,任意有限扩张 E/F 由非分歧扩张 E'/F 和全分歧扩张 E/E' 构成(设 $\overline{E}/\overline{F}$ 可分),每个都是单扩张. 现在,

全分歧部分 E/E' 将再分为顺分歧扩张 V/E' 和野分歧扩张 E/V.

定理 1　E/F 为 e 次完全顺分歧扩张当且仅当 $E=F(\sqrt[e]{\pi})$,其中 π 是 F 的素元且正整数 e 与 p 互素.

证　$\Leftarrow$:由 $\sqrt[e]{\pi}^e=\pi$ 知 $ev_E(\sqrt[e]{\pi})=v_E(\pi)=e(E/F)$,故

$$e\leqslant e(E/F)\leqslant[E:F]\leqslant e.$$

即知 $p\nmid e=e(E/F)=[E:F]$.

$\Rightarrow$:设 π_E 和 π_F 是 E 和 F 的素元,则 $\pi_E{}^e=\pi_F\mu$,其中 $\mu\in U_E$. 由 $\overline{E}=\overline{F}$ 知有 $u\in U_F$ 使 $\overline{u}=\overline{\mu}$. 于是 $\pi_E{}^e=\pi_Fu+\pi_F(\mu-u)$. 我们要证明 π_Fu 可作为定理中的 π,需如下引理.

引理 1　若 $a\in F^*$ 且 $(m,p)=1$,则 $f(X)=X^m-a$ 在 Ω 中的根 $\alpha_1,\cdots,\alpha_m$ 互异,且

$$v(\alpha_i-\alpha_j)=v(\alpha_1),\qquad(1\leqslant i\neq j\leqslant m).$$

进而设有 $\alpha\in E$ (E 为 F 某有限扩张)满足 $v_E(\alpha)>v_E(a)$,且 $g(X)=X^m-a-\alpha$ 有一根 $\beta\in E$,则 $\alpha_1,\cdots,\alpha_m$ 中有某 α_o 使

$$F(\alpha_o)\subset F(\beta)\subset E,$$

且

$$v_E(\alpha_o)=v_E(\beta).$$

由引理 1 可完成定理 1 的证明:令 $\pi=\pi_Fu=a$, $\pi_F(\mu-u)=\alpha$, $m=e$. 则 $g(X)=X^e-a-\alpha$ 有根 $\beta=\pi_E\in E$. 故存在 $X^e-\pi$ 一根 $\alpha_o=\sqrt[e]{\pi}$ 使 $E'=F(\sqrt[e]{\pi})\subset E$ 且 $ev_{E'}(\sqrt[e]{\pi})=v_{E'}(\pi)=$

$e(E'/F)$，故 $e \leqslant e(E'/F)$，从而 $e \leqslant e\ (E'/F) \leqslant [E':F] \leqslant [E:F]=e$，故均为等号，即知$F(\sqrt[e]{\pi})=E$.

引理 1 之证 由 $\alpha_i^m=a$ 知 $m\,v(\alpha_i)=v(a)$，故 $v\,(\alpha_i)=v(\alpha_1)$ $(1\leqslant i\leqslant m)$. 故知$v(\alpha_i-\alpha_j)\geqslant v(\alpha_1)$. 而

$$f'(\alpha_1)=m\alpha_1{}^{m-1}=(\alpha_1-\alpha_2)\cdots(\alpha_1-\alpha_m)$$

$$(m-1)v(\alpha_1)=v(\alpha_1-\alpha_2)+\cdots+v(\alpha_1-\alpha_m)$$
$$\geqslant(m-1)v(\alpha_1),$$

故等号成立，即$v(\alpha_j)=v(\alpha_1)$且$v(\alpha_1-\alpha_j)=v(\alpha_1)(1\leqslant j\leqslant m)$. 同理可知$v(\alpha_i-\alpha_j)=v(\alpha_i)=v(\alpha_j)$. 再注意由 $g\,(\beta)=0$ 知

$$\alpha=\beta^m-a=\prod_i\,(\beta-\alpha_i),$$

故

$$\sum_{i=1}^{m} v(\beta-\alpha_i)=v(\alpha)>v(a)=m\,v(\alpha_j).$$

故至少有一个 i 使得

$$v(\beta-\alpha_i)>v(\alpha_j)=v(\alpha_i).$$

记此 $\alpha_i=\alpha_o$，由 Krasner 引理知$F(\alpha_o)\subset F(\beta)\subset E$. 且$v(\beta)=v(\beta-\alpha_i+\alpha_i)=v(\alpha_i)=v(\alpha_o)$. □

命题 1 (i) 设 E/F 为顺分歧扩张，K/F 为有限扩张，则 EK/K 为顺分歧扩张.

(ii) 若 E/F 和 K/F 均为顺分歧扩张，则 EK/F 为顺分歧扩张.

证 设 E' 为 E/F 的惯性域，则 $E'K/K$ 是非分歧的. 由定理 1 可设 $E=E'(\sqrt[e]{\pi'})$，π'是 E' 的素元. 故 $KE=KE'(\sqrt[e]{\pi'})$，故 KE/KE' 顺分歧，故 KE/K 顺分歧. 其余显然. □

定理 2 任一有限扩域 E/F 含有唯一的最大顺分歧子扩域 V/F. V 包含所有顺分歧子扩域(称为 E/F 的**分歧域**). 若 $e=e(E/F)=e_0p^r,(e_0,p)=1$,则

$$[V:E^t]=e_0, \qquad [E:V]=p^r.$$

证 由命题1知 V 的存在性,设 $\overline{E}/\overline{F}$ 可分,则 E/E^t 为 e 次全分歧扩张. 在定理1证明的第二部分,换 e 为 e_0,换 π_E 为 $\pi_E^{p^r}$,F 为 E^t,则可得到 $v_E(\alpha_0)=v_E(\beta)$, $E^t(\alpha_0)\subset E^t(\beta)\subset E$, $e_0\leqslant e(E^t(\alpha_0)/E^t)\leqslant[E^t(\alpha_0):E^t]\leqslant e_0$,故 $W=E^t(\alpha_0)=E^t(\sqrt[e_0]{\pi})$ 为 E^t 的 e_0 次顺分歧扩张. 当 $\overline{E}/\overline{F}$ 不可分时可类似证明,但应注意 $[E:V]=p^r[\overline{E}:\overline{F}]_i$,其中$[\;]_i$ 指不可分次数. □

习 题

1 考虑 $\boldsymbol{Q}_p$,设 ζ 为 $n=p^s$ 次本原单位根,试证明 $\boldsymbol{Q}_p(\zeta)/\boldsymbol{Q}_p$ 为完全分歧扩张,$1-\zeta$ 为素元,何时此扩张是野分歧的. V 是什么?

§5.5 整体域与局部域

第三章中的分解群和惯性群及其性质,对整体域和局部域的 Galois 扩张都是成立的(局部域时的分解群等于整个 Galois 群). 现在讨论二者的联系.

设 L/K 为整体域的 n 次 Galois 扩张,$G=\mathrm{Gal}(L/K)$. 设 v 是 K 的 $\wp$-adic 赋值,w 是 v 到 L 的一个延拓 $\mathfrak{P}$-adic 赋值,K_v 和 L_w 是相应的完备化. 设 K 是 Dedekind 环 $A=O_K$ 的分式

域，$B=O_L$ 是 A 在 L 的整闭包．我们以 $\wp_v$ 和 $\mathfrak{P}_w$ 记 K_v 和 L_w 的素理想．常设所有的扩张都是可分的．注意我们有

$$L_w=K_vL,$$

故 L_w/K_v 也是 Galois 扩张，且 $\mathfrak{P}\,|\,\wp$ 的分解群 $D(\mathfrak{P}\,|\,\wp)=G_{\mathfrak{P}}$ 与 $G_w=\mathrm{Gal}\,(L_w/K_v)$ 有自然同构(§4.8 系 6)$\varphi=\varphi_{(L/K)}$，即

$$\varphi:\ G_{\mathfrak{P}}\cong G_w,\ \sigma\longmapsto\tilde{\sigma}.$$

而且此同构也使 $\mathfrak{P}$ 和 $\mathfrak{P}_w$ 的惯性群相互同构，

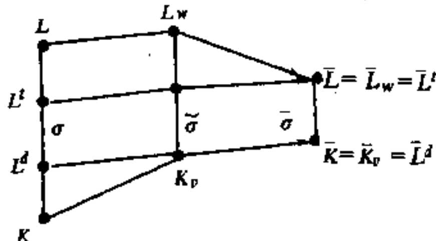
$$\varphi:\ T\,(\mathfrak{P}\,|\,\wp)\cong T\,(\mathfrak{P}_w\,|\,\wp_v)$$

事实上，若 $\sigma\in T_w=T\,(\mathfrak{P}_w\ \wp_v)$，则 $\sigma\alpha\equiv\alpha\,(\mathrm{mod}\mathfrak{P}_w)$ 对任意 $\alpha\in O_w$（即 w 的赋值环）成立．也可写为 $(\sigma-1)\,O_w\subset\mathfrak{P}_w$. 从而 $(\sigma-1)O_L\subset\mathfrak{P}$（因为 $\mathfrak{P}=\mathfrak{P}_w\cap O_L$），即知 σ（到 L 的限制）属于 $T_{\mathfrak{P}}=T(\mathfrak{P}\,|\,\wp)$. 反之，注意 O_w 是 O_L 在 L_w 的闭包，$\mathfrak{P}_w$ 是 $\mathfrak{P}$ 在 L_w 的闭包(见§4.6). 也就是说 O_L 在 O_w 中稠密，$\mathfrak{P}$ 在 $\mathfrak{P}_w$ 中稠密，对于 $\sigma\in T_{\mathfrak{P}}\subset G_{\mathfrak{P}}$，$\sigma$ 按连续性定义为 O_w 中的(连续)映射 $\tilde{\sigma}$. 因 $\mathfrak{P}_w$ 是闭集(§4.6)，故由 $(\sigma-1)O_L\subset\mathfrak{P}$ 即知 $(\tilde{\sigma}-1)O_w\subset\mathfrak{P}_w$，即 $\tilde{\sigma}\in T_w$.

以后我们不再区分 σ 和 $\tilde{\sigma}$，即视二者等同，于是

$$G_{\mathfrak{P}}=G_w,\qquad T_{\mathfrak{P}}=T_w.$$

由整体域 L/K 向局部域 L_w/K_v 过渡时，中间域也都表现很好. 设 E 是 L/L^d 的中间域(当然若 $F\subset L^d$ 则 F 的完备化等



于 K_v，见 §4.8)，设 $\mathfrak{P}_E=\wp\cap E$，则 E 对 $\mathfrak{P}_E$－adic 赋值的完备化 $\tilde{E}=EK_v$ 是 L_w/K_v 的中间域，分解群 $D(\mathfrak{P}|\mathfrak{P}_E)=G(L/E)$. 现由自然同构 $G_{\mathfrak{P}}\cong G_w$，限制到 $D(\mathfrak{P}|\mathfrak{P}_E)=G(L/E)$，则 $G(L/E)=D(\mathfrak{P}|\mathfrak{P}_E)\cong\{\sigma\in G_w|\sigma$ 不变 E 中元$\}=\{\sigma\in G_w|\sigma$不变 $\tilde{E}$中元$\}=G(L_w/\tilde{E})$. 所以，L/K 所对应同构 $\varphi_{(L/K)}$到 E 的限制，与 L/E 对应的同构 $\varphi_{(L/E)}$，二者是一致的.

现取 $E=L^t$，记 $\tilde{E}$的素理想为$\tilde{\mathfrak{P}}_E$(即 $\mathfrak{P}_E$ 的闭包). 则惯性群 $T(\mathfrak{P}|\mathfrak{P}_E)=G(L/L^t)=D(\mathfrak{P}|\mathfrak{P}_E)$. 与上述同样可知 $G(L_w/L_w^t)=T(\mathfrak{P}_w|\tilde{\mathfrak{P}}_E)=G(L_w/\tilde{E})$. 这说明惯性域 $E=L^t$ 的完备化 $\tilde{E}$即为 L_w 的惯性域 L_w^t.

由于 $L_w=K_vL$，故 $G(L_w/K_v)\cong G(L/L\cap K_v)=G(L/L^d)$，故 $L^d=L\cap K_v=L\cap\tilde{L}^d$ ($\tilde{L}^d$表示 L^d 的完备化). 同样可知 $E=L\cap\tilde{E}$对任一中间域 E 成立.

由于有自然同构 φ，且中间域在此同构下有良好表现，所以本章关于局部域的许多讨论对整体域也有平行的结论. 反之也一样. 我们在 §5.2 等处常用的 $G(L/K)$到剩余类域群 $G(\bar{L}/\bar{K})$的同态：$\sigma\longmapsto\bar{\sigma}$，与自然同构 φ 很和谐，由于 $\bar{L}/\bar{K}$ 与 $\overline{L_w}/\overline{K_v}$ 可以等同，故 $\sigma\in G_{\mathfrak{P}}$ 与 $\tilde{\sigma}\in G(L_w/K_v)$到 $G(\bar{L}/\bar{K})=G(\overline{L_w}/\overline{K_v})$有同一个象 $\bar{\sigma}=\bar{\tilde{\sigma}}$.

习　题

1　设 E 为局部域 n 次扩张 L_w/K_v 的中间域，$H=G(L_w/E)$，$G_w=G(L_w/K_v)$，$\overline{G_w}=G(\overline{L_w}/\overline{K_v})$，$\bar{H}=G(\overline{L_w}/\bar{E})$. T_w 为 L_w/K_v 的惯性群，则

$$f(L_w/K_v)=(\overline{G_w}:\bar{H})=(G_w/T_w:HT_w/T_w)$$

$$=(G_w : HT_w),$$

$$e(L_w/K_v)=n/f(L_w/K_v)=(HT_w : H)$$

$$=(T_w : H\cap T_w).$$

特别知 HT_w 的固定域为 E/K_v 的惯性域．

§5.6 差 分

以下三节内容不限于完备域情形．我们利用赋值论继续深入讨论差分和判别式．

以下总设 L/K 是 n 次可分扩张，K 是 Dedekincl 环 A 的分式域，B 是 A 在 L 中的整闭包，并设剩余类域 $\overline{L}/\overline{K}$ 也是可分的．记 $T_r=T_{rL/K}$，$N=N_{L/K}$．因此这里的 L/K 可包括完备域，数域和代数函数域等的可分扩张情形．因 L/K 可分，故这时总可取得 $\alpha\in B$ 使 $L=K(\alpha)$，设 $f(X)=X^n+\cdots+a_1X+a_0=(X-\alpha_1)\cdots(X-\alpha_n)$是 α 在 K 上的极小多项式，记 $\alpha=\alpha_1$，$a_n=1$．记

$$\mathscr{D}_{L/K}(\alpha)=f'(\alpha)=(\alpha-\alpha_2)\cdots(\alpha-\alpha_n),$$

称为 α（对于 L/K）的**差分**(different)．我们已知有

$$N(\alpha)=(-1)^{n(n-1)/2}\mathrm{Disc}\,(1,\alpha,\cdots,\alpha^{n-1}).$$

对于 L 的子集 M，定义

$$M^*=\{\alpha\in L\,|\,T_r(\alpha M)\subset A\},$$

称为 M 的**补集**(complementary set)．显然若 $M_1\subset M_2$ 则 $M_1^*\supset M_2^*$，若 M 为 B-模则 M^* 也是 B-模．且 $B^*\supset B$（因为对 $\alpha,\beta\in B$ 有 $T_r(\alpha\beta)\in A$）．

命题 1 设 $\{\alpha_i\}$ 与 $\{\alpha_i^*\}$ 是 L/K 的互为对偶的基（即 $T_r(\alpha_i\alpha_j^*)=\delta_{ij}$）．则 $M=A\alpha_1+\cdots+A\alpha_n$ 的补集为 $M^*=A\alpha_1^*+\cdots+A\alpha_n^*$．且 $(M^*)^*=M$．

证 每个 $\beta\in L$ 可写为 $\beta=\Sigma b_i\alpha_i^*$ $(b_i\in K)$. 于是 $\beta\in M^*\Leftrightarrow$ $T_r(\beta M)\subset A\Leftrightarrow Tr(\beta\alpha_i)\subset A$ $(1\leqslant i\leqslant n)\Leftrightarrow b_i\in A$ $(1\leqslant i\leqslant n)$. □

由此易知,若 M 为 L 的分式理想则 M^* 也是分式理想,因为分式理想就是有"公分母"的 A-模,是两个形如 $A\alpha_1+\cdots+A\alpha_n$ 的模的中间模.

定义 1 $(B^*)^{-1}$称为 B/A (或 L/K)的差分(different),记为 $\mathscr{D}_{B/A}$(或 $\mathscr{D}_{L/K}$,$\mathscr{D}(L/K)$,$\mathscr{D}$).(注意 $\mathscr{D}$ 是 L 的整理想).

命题 2 设如本节开始. (1)(Euler 引理)$\{1,\alpha,\cdots,\alpha^{n-1}\}$的(相对于 T_r 的)对偶基为$\{\beta_0/f'(\alpha),\cdots,\beta_{n-1}/f'(\alpha)\}$,其中 $\beta_j=\sum\limits_{i=j+1}^{n}a_i\alpha^{i-j-1}$是$f(X)/(X-\alpha)$的 j 次系数.

(2) 若 $M=A[\alpha]=A\cdot 1+A\alpha+\cdots+A\alpha^{n-1}$,则

$$A[\alpha]^*=A[\alpha]/f'(\alpha),$$

$$A[\alpha]\subset B\subset B^*\subset A[\alpha]^*=\frac{A[\alpha]}{f'[\alpha]}.$$

(3) 设 I 为 K 的分式理想,则

$$I^*=B^*I^{-1}.$$

证 (1)对于 $\beta\in E$,记其 K—共轭元为 $\beta^{(i)}$$(1\leqslant i\leqslant n)$,$\beta^{(1)}=\beta$. 于是

$$\frac{f(X)}{X-\alpha_i}=\beta_0^{(i)}+\beta_1^{(i)}X+\cdots+\beta_{n-1}^{(i)}X^{n-1},$$

$$f'(\alpha_i)=\prod_{j\neq i}(\alpha_i-\alpha_j)=\beta_0^{(i)}+\beta_1^{(i)}\alpha_i+\cdots+\beta_{n-1}^{(i)}\alpha_i^{n-1}.$$

由 Lagrange 插值公式知，当 $0\leqslant r\leqslant n-1$ 时有

$$\sum_{i=1}^{n}\frac{f(X)}{(X-\alpha_i)f'(\alpha_i)}\alpha_i{}^r=X^r,$$

比较 X^j 的系数得

$$\sum_{i=1}^{n}\left(\frac{\beta_j^{(i)}}{f'(\alpha_i)}\alpha_i^r\right)=\delta_{rj}.$$

即 $T_r(\alpha^r\cdot\beta_j/f'(\alpha))=\delta_{rj}$. 即得对偶基的结果. β_j 可由下式读出($a_n=1$)：

$$\begin{aligned}&\beta_0+\cdots+\beta_{n-1}X^{n-1}=f(X)/(X-\alpha)\\&=\sum_{1}^{n}a_i\left(\frac{X^i-\alpha^i}{X-\alpha}\right)\\&=a_1+a_2(X+\alpha)+\cdots+a_n(X^{n-1}+\alpha X^{n-2}+\cdots+\alpha^{n-1}).\end{aligned}$$

(2) 由(1)和命题 1 知 $A[\alpha]^*=A\beta_0/f'(\alpha)+\cdots+A\beta_{n-1}/f'(\alpha)$，再由 β_j 的公式即知.

(3) 由 $T_r(B^*I^{-1}I)=T_r(B^*B)\subset A$ 知 $B^*B^{-1}\subset I^*$. 反方向同样显然. □

若 $B=A[\alpha]$，即$\{1,\alpha,\cdots,\alpha^{n-1}\}$是 L/K 的整基(即 B 的 A—基)，则命题 2 (2)说明 $B^*=f'(\alpha)^{-1}B=(f'(\alpha))^{-1}$，即

$$\mathscr{D}=(f'(\alpha))$$

是由$(f'(\alpha))$生成的主理想.

以下我们加上足标，记上述 B^* 为 $B^*_{L/K}$，以便于处理多个域扩张.

命题 3 (差分的链性) 设 $K\subset L\subset M$ 是两个有限可分扩张，B 和 C 是 A 在 L 和 M 中的整闭包，则

(1) $C^*_{M/K}=C^*_{M/L}B^*_{L/K}$，

(2) $\mathscr{D}_{M/K}=\mathscr{D}_{M/L}\mathscr{D}_{L/K}$.

证(1) $\supset$:

$$\begin{aligned}
&Tr_{M/K}(左\cdot C)\\
=&Tr_{L/K}Tr_{M/L}(左\cdot C)\\
=&Tr_{L/K}(B^*_{L/K}Tr_{M/L}(C^*_{M/L}C))\\
\subset&Tr_{L/K}(B^*_{L/K}B)\subset A.
\end{aligned}$$

$\subset$: 设 $\gamma\in C^*_{M/K}$则

$$A\supset Tr_{M/K}(\gamma C)=Tr_{L/K}(BTr_{M/L}(\gamma C)),$$

(因 $BC=C$ 故可插入 B),故知 $Tr_{M/L}(\gamma C)\subset B^*_{L/K}$,从而

$$B^{*-1}_{L/K}Tr_{M/L}(\gamma C)\subset B,$$

注意 $B^{*-1}_{L/K}$属于 L,故知

$$Tr_{M/L}(B^{*-1}_{L/K}\gamma C)\subset B,$$

即知
$$\gamma B^*_{L/K}\subset C^*_{M/L}.$$
即
$$\gamma\in C^*_{M/L}B^*_{L/K}.$$

(2) 由(1)取逆即得. □

以下将建立整体域与局部域的差分的关系. 为此注意,若 K 中理想 I 分解为 $I=\wp_1^{a_1}\cdots\wp_s^{a_s}$,则整数 $a_1,\cdots,a_s$ 唯一决定理想 I. 因此引入"**形式**"**理想**的概念,也就是说,不同域的理想可以认为是相同的(形式理想意义下). 详言之,设 I_1 和 I_2 为环 A_1 和 A_2 的理想,环 R 包含 A_1 和 A_2,若 $I_1R=I_2R$,则称 $I_1=I_2$. 特别,设$\wp$是 Dedekind 环 A 的素理想,K 是 A 的分式域,A'是 A 的分式环(例如 $A'=A_\wp$ 是 A 对$\wp$的局部化),K_v 是 K 对 $\wp$-adic 赋值 v 的完备化,A_v 是 A 在 K_v 的闭包(也是 K_v 的赋值环). 则 $A\subset A'\subset A_v$, $\wp\subset\wp A'\subset\wp A_v=\wp_v$. 我们可形式地记

为

$$\wp=\wp A'=\wp_v.$$

当然对于 L 及其理想 $\mathfrak{B}$ 和 $\mathfrak{B}$-adic 赋值 w 有同样定义．以下将证明，B，B'和 B_w 的差分的 $\mathfrak{B}$—分量是相等的．而后者易求，因为是主理想环上模．首先显然有

命题 4 设 S 是 A 的一个乘法闭子集，则

$$\mathscr{D}_{S^{-1}B/S^{-1}A}=S^{-1}\mathscr{D}_{B/A}.$$

也就是说，差分的分式环等于分式环的差分，下面的命题适用于 A'为 $A_\wp$(局部化)的情形．

命题 5 设 A'是离散赋值环，v 是其赋值，$\wp$ 为其素理想，K 是 A'的分式域，L/K 为有限扩张，B 为 A'在 L 的整闭包，$\mathfrak{B}$ 为 $\wp$ 在 L 中的素理想因子，w 是 $\mathfrak{B}$—adic 赋值，K_v 和 L_w 为对 v 和 w 的完备化，$A_v=A'_v$ 和 B_w 是 A'和 B 的完备化．则作为 B_w 的理想有

$$(\mathscr{D}_{B/A'})=\mathscr{D}_{B/A'}B_w=\mathscr{D}_{B_W/A_v}.$$

证 只需证 B^* 在 B_w^* 中稠密．记 Tr 为 L 到 K 的迹，Tr_w 为 L_w 到 K_v 的迹．设 $x\in B_w^*$，即 $x\in L_w$ 使 $\mathrm{Tr}_w(xB_w)\subset A_v$. 选取 $s\in L$，使 s 在 w 接近 x，在其它 $\varphi|v$ 接近于 0. 设 $y\in B$，则 $\mathrm{Tr}_\varphi(sy)$接近 0 (若 $\varphi\neq w$)，$\mathrm{Tr}_w(sy)\in A_v$. 这说明 $\mathrm{Tr}(sy)\in A$. 故 $s\in B^*$.

反之，设 $x\in B^*$，$y\in B_w$. 取 $s\in L$ 在 w 接近 x，在其余 $\varphi|v$ 接近 0，于是

$$\mathrm{Tr}(st)=\mathrm{Tr}_w(st)+\sum_{\varphi\neq w}\mathrm{Tr}_\varphi(st).$$

左边属于 A，右边和号下各项属于 A_v. 故 $\mathrm{Tr}_w(st)\in A_v$. 因 s，t

分别近于 x 和 y，故 $\mathrm{Tr}_w(xy)$ 也属于 A_v，即 $x\in B_w^*$. 命题得证.

□

在命题 4 中取 $S=B-\mathfrak{B}$，其中 $\mathfrak{B}$ 为 B 的素理想，$B'=S^{-1}B$，则知局部化环 B'/A' 的差分 $\mathscr{D}_{B'/A'}$ 等于整体差分 $\mathscr{D}_{B/A}$ 的 $\mathfrak{B}$-分量. 而命题 5 说明 $\mathscr{D}_{B'/A'}=\mathscr{D}_{B_w/A'}=\mathscr{D}_{\mathfrak{B}}$，即完备化(局部)环 B_w/A_v 的差分. 因此我们有(形式理想)等式：

$$\mathscr{D}_{L/K}=\coprod_{\mathfrak{B}}\mathscr{D}_{\mathfrak{B}}\quad(\mathfrak{B}\text{ 过 } L \text{ 的素理想}).$$

即**整体差分** $\mathscr{D}$ 是各**局部差分** $\mathscr{D}_{\mathfrak{B}}$ 的积，$\mathscr{D}_{\mathfrak{B}}$ 可解释为 $\mathscr{D}$ 的 $\mathfrak{B}$-分量，或局部化环的差分，或完备化环的差分.

习　　题

1. 设 L/K 如本节初. I 为 L 的分式理想，I^* 为其补集，则
   (1) $B^*\supset B$ 且是 L 的理想.
   (2) $\mathrm{Tr}\,(I)\subset A\Leftrightarrow I\subset B^*$.
   (3) $(B^*)^{-1}$是 B 的整理想.
   (4) I 是 B 的整理想$\Leftrightarrow(I^*)^{-1}\subset(B^*)^{-1}$.
   (5) $(I^*)^*=I$.
   (6) $\mathrm{Tr}B^*=A$.
   (7) $B^*=\mathrm{Tr}^{-1}(A)$.

§5.7　差分与分歧

设 $L\supset K$ 为 n 次可分扩张如上节开始，且设 $\wp$ 为 K 的素理想，$\overline{K}=A/\wp$ 是完全域. 设 $\mathfrak{B}$ 是 $\wp$ 在 L 中的素理想因子，设 $v=v_\wp$，$w=v_{\mathfrak{B}}$ 是标准指数赋值(即$v(K^*)=\mathbf{Z}=w(L^*)$)，$e=$

$e(\mathfrak{P}|\wp)$，$\mathscr{D}=\mathscr{D}_{L/K}$为 L/K 的差分.

定理 1 设 $\mathfrak{P}^m \| \mathscr{D}$，则当且仅当 $m\geqslant 1$ 时 $\mathfrak{P}$ 在 L/K 分歧，且

(i) $\mathfrak{P}$ 对 L/K 顺分歧$\Leftrightarrow m=e-1$；

(ii) $\mathfrak{P}$ 对 L/K 野分歧$\Leftrightarrow e\leqslant m\leqslant e-1+v_{\mathfrak{P}}(e)$；

(iii) $\mathscr{D}=\gcd_{\alpha}(f'(\alpha))$，$\alpha\in B$ 在 K 上生成 L，$f(X)$为 α 的 n 次不可约多项式.

证 由上节知 $\mathfrak{P}^m=\mathscr{D}_w$（完备化域 L_w/K_v 的差分）. 由 §5.3 定理 2 知完备域扩张 L_w/K_v 有整基$\{1,\alpha,\cdots,\alpha^{n_1}\}$，且 α 是 L_w 的单位. 于是 L_w 的整数环 $B_w=A_v[\alpha]$. 设 α 在 K_v 上极小多项式为$f(X)$，则

$$\mathfrak{P}^m=\mathscr{D}_w=(f'(\alpha)),\ m=w(f'(\alpha)).$$

若 $\mathfrak{P}$ 非分歧，则由 §5.2 可知 $\bar{\alpha}$ 是 $\bar{f}(X)$的单根，故 $f'(\alpha)\in U_w$(单位群)，故 $m=0=e-1$，$\mathscr{D}_w=(1)$.

再设 $\mathfrak{P}$ 完全分歧，$e=n_1=[L_w:k_v]$. 由 §5.3 知 α 可取为 L_w 的素元 π，其极小多项式为 Eisenstein 多项式：

$$f(X)=X^e+a_1X^{e-2}+\cdots+a_e,$$

$$f'(\alpha)=f'(\pi)=ea_0\pi^{e-1}+(e-1)a_1\pi^{e-1}+\cdots+a_{e-1}.\ (a_0=1)$$

故对 $r=0,1,\cdots,e-1$ 有

$$\begin{aligned}w((e-r)a_r\pi^{e-r-1})&=ev(e-r)+ev(a_r)+e-r-1\\&\equiv e-r-1(\bmod e).\end{aligned}$$

这说明 $f'(\pi)$各项的指数赋值不同，故

$$m=w(f'(\pi))=\min\{w((e-r)a_r\pi^{e-r-1})\}.$$

若 $\mathfrak{P}$ 为完全顺分歧，即 $p\nmid e$，p 为 $\overline{K}$ 的特征. 则 $w(e)=0$，

上述极小值为 $e-1$（当 $r=0$）.

若 $\mathfrak{P}$ 为完全野分歧，即 $p|e$，则 $v(e)\geqslant 1$，易得

$$e\leqslant m\leqslant w(e)+e-1.$$

对于 $\mathfrak{P}$ 不完全分歧的情形，设 T 为惯性域，$K_v\subset T\subset L_w$，则

$$\mathscr{D}_w=\mathscr{D}_{L_w/T}\mathscr{D}_{T/K_v}=\mathscr{D}_{L_w/T},$$

即知上述结果仍成立．这证明了(i) 和(ii)．

(iii) 为此要证明，对 L 的任一素理想 $\mathfrak{P}$，存在 L 的生成元 $\alpha=\alpha_{\mathfrak{P}}$ 使得

$$\mathfrak{P}^m \parallel (f'(\alpha))\text{，即 } v_{\mathfrak{P}}(\mathscr{D})=v_{\mathfrak{P}}(f'(\alpha)).$$

当然，若 $B=A[\alpha]$则立得结论．所以我们应用逼近定理归结到局部域情形．

设$\{\sigma\}$是 L 到 Ω(K_v 的代数闭包)的 K—嵌入全体，设 σ_1 是其中之一，诱导出 L 的赋值 $v_{\mathfrak{P}}=w$. 若 α 是 L 在 K 上的生成元，$f(X)$是其在 K 上的极小多项式，则

$$\sigma_1 f'(\alpha)=f'(\sigma_1\alpha)=\prod_{\sigma\neq\sigma_1}(\sigma_1\alpha-\sigma\alpha).$$

以 $\sigma\sim\tau$ 记 σ 和 τ 在 K_v 上共轭，即有 Ω 的 K_v-自同构 λ 使 $\tau=\lambda\sigma$（在 L 上）. 由 § 3 定理 2 知存在 $\beta\in B_w$ 使 $B_w=A_v[\beta]$，注意，任一与 β 充分接近的元素 $\beta'\in B_w$ 也在 A_v 上生成 B_w.

设 λ 遍历 Ω 的 K_v-自同构，则存在 $a\in A_v$ 使

$$|\lambda\beta-a|=1 \qquad (\forall\ \lambda),$$

事实上，诸 $\lambda\beta$ 的剩余类在 $A_v/\wp_v$ 上共轭，若这些共轭类为 0，则可取 $a=1$；若它们非 0 则取 $a=0$ 即可．

设 $\sigma_1,\cdots,\sigma_r$ 是$\{\sigma\}$的共轭等价类代表元系．由逼近定理知，存在 $\alpha\in L$ 使

$$|\sigma_1\alpha-\beta|<\varepsilon, \qquad |\sigma_i\alpha-a|<\varepsilon(i\neq 1).$$

(ε 为充分小正数). 不妨设 α 在 A 上整且 $L=K(\alpha)$(否则可代 α

以 $b\alpha+\pi^s\gamma=\alpha'$，其中 $b\in A$，$b\equiv1(\bmod \wp)$且 $b\alpha$ 在 A 上整；γ 是任一整 L 的生成元，s 充分大）.

因 $\sigma_1\alpha$ 充分接近 β，故 $B_w=A_v[\sigma_1\alpha]$，从而 L_w/K_v 的差分的指数赋值

$$v_{\mathfrak{P}}(\mathscr{D}_w)=v_{\wp}\prod_{\substack{\sigma\sim\sigma_1\\ \sigma\neq\sigma_1}}(\sigma_1\alpha-\sigma\alpha).$$

只需要再证明其余的因子对 $\mathfrak{P}$-分量无贡献．设 σ 与 σ_1 在 K_v 上不共轭，记 $\sigma=\lambda\sigma_i(i\neq1)$，则

$$\begin{aligned}|\sigma_1\alpha-\sigma\alpha|&=|\sigma_1\alpha-\lambda\sigma_i\alpha|=|\lambda^{-1}\sigma_1\alpha-\sigma_i\alpha|\\&=|\lambda^{-1}\sigma_1\alpha-a+a-\sigma_i\alpha|\end{aligned}$$

注意 $|\sigma_i\alpha-a|$ 很小，$\lambda^{-1}\sigma_1\alpha$ 非常接近 $\lambda^{-1}\beta$. 由 $|\lambda^{-1}\beta-a|=1$ 知 $|\lambda^{-1}\sigma_1\alpha-a|=1$. 故 $|\sigma_1\alpha-\sigma\alpha|=1$. □

§5.8 判别式

仍设 L/K 如 §5.6 开始，$B\supset A$ 分别为其中整环．

在 §1.4 中已讨论了元素的判别式，在 §1.5，当 L/K 有相对整基（即 B 的 A－基）$\alpha_1,\cdots,\alpha_n$ 时，定义（$\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)$）为 L/K 的判别式 $\mathrm{Disc}(L/K)=D(L/K)$. 现将此定义稍作扩充．若 $M\subset L$ 为 A—模，且有 A—基 $\alpha_1,\cdots,\alpha_n$，即

$$M=A\alpha_1+\cdots+A\alpha_n,$$

则 $\mathrm{Disc}(\alpha_1,\cdots,\alpha_n)$生成的理想称为 M 的判别式 $\mathrm{Disc}(M)=D(M)$. 特别当 A 为主理想整环时（即 K 的理想类数为 1），M 总有 A—基，总可以这样定义判别式．此定义特别对 L 的理想 M 适用. 上述 $D(L/K)$不过就是 $D(B)$（以下常将 Disc 省记为 D）.

但在一般情形下，A—模不一定有 A—基（即不一定是自由

模)。上述定义不再适用.

一般地，L 的分式理想 I **的判别式** $D_{L/K}(I)$ 定义为所有 $D_{L/K}(\alpha_1,\cdots,\alpha_n)$ 生成的理想，其中 $\alpha_i\in I$. L/K **的判别式**就定义为 B 的判别式：$D(L/K)=D_{L/K}(B)$，即 $\{D_{L/K}(\alpha_1,\cdots,\alpha_n)\mid\alpha_i\in B\}$ 生成的理想. 当然这样定义的判别式不易计算，我们将证明它等于各局部域判别式的积. 首先由定义易知有如下命题，它使我们可以用局部化方法：

命题 1 设 I 为 L 的分式理想，S 是 A 的乘法封闭集. 则

$$S^{-1}D_{L/K}(I)=D_{L/K}(S^{-1}I).$$

由此可知，若 $\wp$ 是 A 的素理想，则可在 $\wp$ 局部化而计算判别式的 $\wp$ 一分量.

命题 2 (1) 设 I 是 B 的分式理想，则 I 对 L/K 的判别式满足

$$D(I)=N(I)^2D(L/K),$$

其中 N 是理想的从 L 到 K 的范映射.

(2) 设 A 还是离散赋值环，I 是 B 的分式理想，于是 $I=(\beta)$，$\beta\in L$. 则

$$D(I)=N(\beta)^2D(L/K).$$

证 先证(2)，这实际上是局部情形. 设 $\alpha_1,\cdots,\alpha_{n_1}$ 是 B 的 A-基，则 $\{\beta\alpha_i\}$ 是 I 的 A-基. 由判别式定义即得.

再证(1) 只需对 A 的每个素理想 $\wp$ 验证两边的 $\wp$-分量. 由命题 1(令 $S=A-\wp$)，则可设 A 为离散赋值环(即 $S^{-1}A=A_\wp$). 于是由(2)即知. □

定理 1 (1)差分的范即为判别式：

$$N_{L/K}(\mathscr{D}_{L/K})=D(L/K)$$

(2) 整体扩张的判别式等于各局部扩张判别式的积：

$$D(L/K)=\coprod_{w} D(L_w/K_v).$$

其中 $w=w_{\mathfrak{P}}$ 为 $\mathfrak{P}$—adic 赋值，$\mathfrak{P}$ 过 L 的素理想.

(3)(判别式的链性)设 $K\subset L\subset M$ 为两个有限可分域扩张，则

$$D(M/K)=N_{L/K}D(M/L)\cdot(D(L/K))^{[M:L]}.$$

证 (1)由§5.6命题4和本节命题1(取 $S=A-\wp$)，结论归结到 A 为离散赋值环情形. 因此 B 是自由 A-模，设 $\{\alpha_i\}$ 为其 A—基，则 $D(L/K)=D(B)=(D\{\alpha_i\})$. 设 $\{\alpha_i^*\}$ 是 $\{\alpha_i\}$ 的对偶 K-基，则 $\{\alpha_i^*\}$ 是 B^* 的 A-基(§5.命题1)，故

$$D(B^*)=(D\{\alpha_i^*\}).$$

但

$$D\{\alpha_i\}\cdot D\{\alpha_i^*\}=(1)=A,\ (\S 1.4)$$

故

$$D(B)\cdot D(B^*)=(1)=A.$$

再由命题2知 $D(B^*)=N(B^*)^2D(L/K)=N(\mathscr{D})^{-2}D(L/K)$，即得所欲证.

(2) 考虑 $\mathscr{D}=\coprod_{\mathfrak{P}}\mathscr{D}_{\mathfrak{P}}$，其中 $\mathscr{D}_{\mathfrak{P}}=\mathfrak{P}^m$ 是 $\mathscr{D}$ 的 $\mathfrak{P}$-分量. 于是 L_w/K_v 的差分 $\mathscr{D}_w=\mathfrak{P}_w^m$($\mathfrak{P}_w$ 是 $\mathfrak{P}$ 在 L_w 的闭包). 由(1)知

$$N(\mathscr{D})=\coprod_{\mathfrak{P}} N\mathscr{D}_{\mathfrak{P}}=\coprod_{\mathfrak{P}} N\mathfrak{P}^m=\coprod_{\mathfrak{P}}\ \wp^{mf}.$$

其中 $f=f(\mathfrak{P}\mid\wp)=f(\mathfrak{P}_w\mid\wp_v)$，(因为 $f(\mathfrak{P}\mid\wp)=[\overline{L}:\overline{K}]=[\overline{L}_w:\overline{K}_v]=f(\mathfrak{P}_w\mid\wp_v)$)，而由(1)同样知道：

$$\mathrm{Disc}(L_w/K_v)=N_w(\mathscr{D}_w)=N_w\mathfrak{P}_w^m=\wp_v^{mf}.$$

由于$\wp_v$视为等同于$\wp$（定理中相等的意义即如此），即得(2)。

(3) 由§5命题3中差分的链性和(1)即得． □

系1 设$\alpha\in B$，$\wp$为A的素理想，若$\wp\nmid(D(\alpha)/D(L/K))$，则$B_\wp=A_\wp[\alpha]$（其中$B_\wp=(A-\wp)^{-1}B$，$A_\wp=(A-\wp)^{-1}A$）．

证 因$A_\wp$是主理想环，故$B_\wp$作为$A_\wp$-模是自由的，设$B_\wp=A_\wp w_1+\cdots+A_\wp w_n$．由题设知

$$D(\alpha)=D(B)\cdot c^2,$$

$p\nmid c^2$，即c是$A_\wp$中单位，也就是说两边作为$A_\wp$中的理想是相等的．由命题1知，作为$A_\wp$的理想有$D(\alpha)=D(B)=D(B_\wp)=D(\{w_i\})$，故知$1,\alpha,\cdots,\alpha^{n-1}$是$B_\wp$的$A_\wp$-基，即$B_\wp=A_\wp[\alpha]$．

□

系2 设K_1,K_2为m,n次数域，绝对判别式$D(K_1)$与$D(K_2)$互素，且K_1K_2为mn次域，则

(1) 绝对差分$\mathscr{D}(K_1K_2)=\mathscr{D}(K_1)\mathscr{D}(K_2)$；

(2) 绝对判别式$D(K_1K_2)=D(K_1)^nD(K_2)^m$；

(3) 整数环 $O_{K_1K_2}=O_{K_1}O_{K_2}$．

证 (1)由差分的链性知

$$\mathscr{D}(K_1)\mathscr{D}(K_1K_2/K_1)=\mathscr{D}(K_2)\mathscr{D}(K_1K_2/K_2).$$

由$D(K_1)=N\mathscr{D}(K_1)$与$D(K_2)$互素，知$\mathscr{D}(K_1)$与$\mathscr{D}(K_2)$互素．由此知另两因子也互素（因若$\wp$在K_1非分歧（即$\wp\nmid\mathscr{D}(K_1)$），则$\wp$在K_1K_2/K_2也非分歧）．故

$$\mathscr{D}(K_1)=\mathscr{D}(K_1K_2/K_2),\qquad \mathscr{D}(K_2)=\mathscr{D}(K_1K_2/K_1).$$

即得(1). 在(1)两边取范 $N_{K_1K_2/Q}=N_{K_1}N_{K_1K_2/K_1}$即可得(2). 取 K_1 的整基$\{w_i\}$, K_2 的整基$\{v_i\}$. 于是对偶基$\{w_i^*\}$生成 $\mathscr{D}(K_1)^{-1}=O_{K_1}^*$, 由上述知$\{w_i^*\}$也生成 $\mathscr{D}(K_1K_2/K_2)^{-1}=O_{K_1K_2}^*$ ($O_{K_1K_2}$视为 O_{K_2}-模). 故$\{w_i\}$生成 $O_{K_1K_2}$(O_{K_2}-模), 亦即$\{w_i\}$在 O_{K_2}上生成 $O_{K_1K_2}$, 即得(3). 顺便指出, 由此可知$\{w_iv_j\}$是 $O_{K_1K_2}$的 $\mathbf{Z}$-基. 由判别式的定义, 计算行列式也可由此得(2). □

例 1 四次循环数域 K 的判别式 $D(K)$可由局部域方法很快得到(见[Zh7]). 记 K 的唯一实二次子域为 $k=\mathbf{Q}(\sqrt{u})$, u 为无平方因子整数, 则四次循环域 K 均可被唯一地表为

$$K=\mathbf{Q}(\sqrt{vw\eta}),$$

其中 $v,w\in\mathbf{Z}$, $(u,v)=1$, $w|u$, $0<w<\sqrt{u}$; $\eta\in k$ 固定(设 $u=a^2+b^2$, a 奇, 则可取 $\eta=(b+\sqrt{u})u$). 故对每个固定 v, 有 2^{g-1}个四次循环域 K 含 k(g 为 u 的素因子个数). 相对判别式

$$D(K/k)=2^{\delta}v\sqrt{u},$$

其中 $\delta=2$ 或 0(仅当 u 与 v 均奇且 $v\equiv(u+1)/2(\bmod 4)$时 $\delta=0$). 有趣的是, 当且仅当 $w=1$ 时, K/k 具有相对整基, 即 O_K 是自由 O_k-模, 此时 K 可写为 $K=\mathbf{Q}(\sqrt{v\varepsilon\sqrt{u}})$, ε是 k 的基本单位.

例 2 对 2^n 次数域 $L=\mathbf{Q}(\sqrt{m_1},\cdots,\sqrt{m_n})$, [Zh1]中给出了整基, 以及判别式:

$$D(L)=(2^t)^{2^{n-1}}\prod_{1\leqslant i\leqslant 2^n-1}m_i=(2^t m)^{2^{n-1}}$$

其中 $\mathbf{Q}(\sqrt{m_i})$($1\leqslant i\leqslant 2^n-1$)是 L 的二次子域全体, m_i 无平方因

子，m 是无平方因子奇数；而当 $(m_1,\cdots,m_n)\equiv(1,\cdots,1),(3,1,\cdots,1),(2,1,\cdots,1),(2,3,1,\cdots,1)\pmod 4$ 时，t 分别为 0,2,2,3；s 分别为 0,2,3,4.

一般地，对于素数幂 q^n 次 Abel 扩域 L[Zh8～9]给出了素分解和判别式等．有趣的是，在一定条件下，L 对其子域 K 的相对判别式 $D(L/K)$ 是有理数的平方生成的主理想，(如当 $q\neq 2$，$[L:K]\geqslant e(p)$（对任意素数 p）时)，而且 L/K 具有相对整基.

习　题

1. 设 $K=\boldsymbol{Q}(\alpha)$ 为五次数域，α 满足 $f(X)=X^5+20X+16$，证明：

(1) $\mathrm{Disc}(1,\alpha,\alpha^2,\alpha^3,\alpha^4)=(5^6 16^4)$，故当 $p\neq 2$ 和 5 时 $\{1,\alpha,\alpha^2,\alpha^3,\alpha^4\}$ 是 K 在 p 的整基．

(2) 3 在 K 惯性，(3) 在 K 中仍为素理想．

(3) 5 在 K 完全分歧：$e=5$.

(4) 7 在 K 有三个素理想因子：$e_1=e_2=e_3=1$，$f_1=f_2=1$，$f_3=3$.

(5) 2 在 K 有二个素理想因子：$e_1=4, e_2=1, f_1=f_2=1$.

(提示：令 $\beta=\alpha^2/2, \gamma=(\alpha^3+2\alpha)/4$，则 $\mathbf{Z}$—模 $M=\mathbf{Z}+\mathbf{Z}\alpha+\mathbf{Z}\beta+\mathbf{Z}\gamma+\mathbf{Z}\beta^2\subset\mathbf{Z}[\alpha]$. 且因 M 在 $\mathbf{Z}$ 上有限生成故 $M\subset O_K$. 考虑 $\gamma-1$ 的极小多项式的 Newton 折线.)

2. 设 L/K 为 n 次 Galois 扩张，I 为 L 的理想，若 $\sigma I=I$ $(\forall\ \sigma\in G(L/K))$，则称 I 为不变理想，此时 I^n 是 K 的理想．证明差分 $\mathscr{D}_{L/K}$ 是不变理想，且

$$N_{L/K}(\mathscr{D}_{L/K})=\mathscr{D}^n_{L/K}=\mathrm{Disc}(L/K).$$

第六章　类数与单位

§6.1　类数的有限性

本节用很直接的方法,证明任一数域 K 的类数 $h(K)$是有限正整数.

设 K 为 n 次数域,A 为其整数环.K 的(或称 A 的)非零分式理想全体记为 $\mathscr{I}(K)$,其中主理想全体记为 $\mathscr{P}(K)$,它们都是乘法群.商群 $H(K)=\mathscr{I}(K)/\mathscr{P}(K)$称为(理想)类群,类群的阶 $h(K)$称为(理想)类数.

引理 1　设 K 为 n 次数域,则存在常数 C(仅依赖于 K),使得 K 的每个理想类中均存在一个整理想 J,其范 $NJ\leqslant C$.

证明　任取一个理想类 $\boldsymbol{a}$,在类 $\boldsymbol{a}^{-1}$中任取一整理想 I(§2.3 系 2).设 $w_1,\cdots,w_n$ 是 A 的 $\mathbf{Z}$-基,令 A 的子集

$$S=\{a_1w_1+\cdots+a_nw_n\mid 0\leqslant a_i\leqslant(NI)^{1/n}+1,a_i\in\mathbf{Z}\}.$$

显然每个 a_i 有多于$(NI)^{1/n}$个取值,S 中元素个数大于 $N(I)=\#A/I$.故存在 α、$\beta\in S$ 使 $\alpha\equiv\beta \bmod I$,即 $\gamma=\alpha-\beta\in I$,亦即 $I\mid(\gamma)$.故有整理想 J 使$(\gamma)=IJ$.注意 J 与 I^{-1}同类,即 J 属于

类 $\boldsymbol{a}$. 又由 α、$\beta\in S$ 知 $|N_{K/Q}(\gamma)|=\prod_{\sigma}|c_1w_1^{\sigma}+\cdots+c_nw_n^{\sigma}|$，其中 $0\leqslant|c_i|\leqslant(NI)^{1/n}+1\leqslant2(NI)^{1/n}$，设 $M=\max_i|w_i|$，即知 $|N_{K/Q}(\gamma)|\leqslant n^n2^n(NI)M^n=CN(I)$（即令 $C=(2nM)^n$）. 于是知 $N(IJ)=|N_{K/Q}(\gamma)|\leqslant CN(I)$，$N(J)\leqslant C$. □

定理1 任一数域 K 的理想类数 $h(K)$ 是有限正整数.

证明 由引理1知，存在常数 C，使 K 的每个理想类中均存在一个整理想 J 满足范 $NJ\leqslant C$. 但是满足 $NJ\leqslant C$ 的 J 只能有有限多个，从而 K 的理想类只能有有限多个.（若 $J=\prod_{\wp}\wp^{n_\wp}$，则 $NJ=\prod_{\wp}p^{f_\wp n_\wp}\leqslant C$，故 p，$n_\wp$ 只有有限个选取，故 J 只有有限个）. □

更精细的分析可以给出 C 的明显上界，从而可以具体定出 J，给出 $h(K)$.

注记 设 $k=\boldsymbol{F}_q(X)$ 为有限域 $\boldsymbol{F}_q$ 上有理式形式域，或称有理函数域，k 的有限扩张 K 称为代数函数域. 定理1对代数函数域 K 也是成立的，证明也类似. 这时 k 的素理想即为不可约多项式 $p(X)\in\boldsymbol{F}_q[X]$ 生成的理想。$\boldsymbol{F}_q[X]$ 在 K 中的整闭包记为 O_K（数域中的 $\boldsymbol{Z}$，$\boldsymbol{Q}$，K，O_K 可类比于代数函数域中的 $\boldsymbol{F}_q[X]$，k，K，O_K）. O_K 是 Dedekind 环，素理想即为 k 的素理想的因子. 理想类群 $H(K)$ 和理想类数 $h(K)$ 的定义与数域时一样. 读者应将这里所说的理想类群 $H(K)$ 与除子类群相区别. 一个理想只是在素理想（对应于有限素除子）上有分量，而一个普通除子是在

每个素除子(包括无限素除子)上有分量.

§6.2 数域的嵌入

设 K 为 n 次数域,M_K 是 K 的素除子集,我们知道

$$M_K=\{\infty_1,\cdots,\infty_r,v_{r+1},v_{r+2},\cdots\}$$

其中 $r=r_1+r_2$, r_1是 K 到 $\boldsymbol{R}$ 的嵌入 $\sigma_1,\cdots,\sigma_{r_1}$的个数, r_2是 K 到 $\boldsymbol{C}$ 的复嵌入 $\sigma_{r_1+1},\bar{\sigma}_{r_1+1},\cdots,\sigma_{r_1+r_2},\bar{\sigma}_{r_1+r_2}$的对数($\bar{\sigma}\alpha=\overline{\sigma\alpha}$),$r_1+2r_2=n$; ∞_i 是无限素除子($1\leqslant i\leqslant r$),v_i 是$\wp_i$—adic 素除子($i>r$). 相应有 K 的完备化

$$K_{\infty_1}=\cdots=K_{\infty_{r_1}}=\boldsymbol{R},\ K_{\infty_{r_1+1}}=\cdots=K_{\infty_r}=\boldsymbol{C},\ K_{v_{r+1}},K_{v_{r+2}},\cdots\cdots.$$

所以我们有嵌入

$$\eta: K\longrightarrow \boldsymbol{R}\times\cdots\times\boldsymbol{R}\times\boldsymbol{C}\times\cdots\times\boldsymbol{C}\times K_{v_{r+1}}\times K_{v_{r+2}}\times\cdots=\prod_{v\in M_K}K_v,$$

$$a\longmapsto(\sigma_1(a),\cdots,\sigma_{r_1}(a),\cdots,\sigma_r(a),\ a,\cdots).$$

这一嵌入可以说包含了 K 的所有数论信息,对研究 K 极为重要. 例如,a 为 K 的单位当且仅当 a 在每个 $K_{v_{r+1}},K_{v_{r+2}},\cdots$的嵌入象均是单位.(当然,任一 $a\in K$ 到各 K_v 的嵌入象几乎都是 K_v 的整数,也几乎都是 K_v 的单位(当 $a\neq 0$时). 因此,上述映射的右方 $\prod_{v\in M_K}K_v$ 显得太大,适当缩小之后,就引入了 adele 和 idele 的重要概念).

特别,我们截取上述嵌入的无限素除子部分,得到嵌入

$$\sigma:\ K\longrightarrow\boldsymbol{R}^{r_1}\times\boldsymbol{C}^{r_2},$$

$$a\longmapsto(\sigma_1(a),\cdots,\sigma_r(a)).$$

这称为 K 到 $\boldsymbol{R}^{r_1}\times\boldsymbol{C}^{r_2}$的**正则嵌入**.

将 $\boldsymbol{C}$ 与 $\boldsymbol{R}^2$等同($a+bi\longrightarrow(a,b)$),则 $\boldsymbol{R}^{r_1}\times\boldsymbol{C}^{r_2}$等同于 $\boldsymbol{R}^n$. 以下将证明 σK 是 $\boldsymbol{R}^n$ 的离散子群,是格. 先讨论 $\boldsymbol{R}^n$ 的格.

$\boldsymbol{R}^n$ 是 $\boldsymbol{R}$ 上的线性空间,自然也是加法群. 设 H 是 $\boldsymbol{R}^n$ 的子群,若 $\boldsymbol{R}^n$ 每个有界子集与 H 的交均是有限集,则 H 称为**离散子群**.

引理1 设 H 为 $\boldsymbol{R}^n$ 的离散子群,则 H 是自由 $\boldsymbol{Z}$-模,即

$$H=\boldsymbol{Z}w_1\oplus\cdots\oplus\boldsymbol{Z}w_r.$$

证 记 H 在 $\boldsymbol{R}$ 上张成的子空间为$[H]$,并设其维数为 r. 若 $r=1$,则$[H]=\boldsymbol{R}w$,$w\in H$. 使 $\lambda w\in H$ 的最小正实数 λ 记为 λ_1,记 $W_1=\lambda_1 W$,则显然 $H=\boldsymbol{Z}w_1$. 设对$[H]$的维数不超过 $r-1$ 的情形引理正确,现看维数为 r 的情形. 设

$$[H]=\boldsymbol{R}w_1\oplus\cdots\oplus\boldsymbol{R}w_r,\quad w_i\in H.$$

记
$$V=\boldsymbol{R}w_1\oplus\cdots\oplus\boldsymbol{R}w_{r-1},$$

由归纳假设知 $H\cap V$ 是自由 $\boldsymbol{Z}$-模,不妨从开始就设 $w_1,\cdots,w_{r-1}$ 为其 $\boldsymbol{Z}$-基. 故

$$H\cap V=\boldsymbol{Z}w_1\oplus\cdots\oplus\boldsymbol{Z}w_{r-1}.$$

对任意 $v\in H$,在不计 $w_1,\cdots,w_r$ 整数倍意义下可设 $v=\sum_1^r c_iw_i$, $0\leqslant c_i<1(0\leqslant i\leqslant r)$. 这样的 v 均在一有界集中,故只有有限多个. 取其中使 $c_r\neq0$最小的一个,记为

$$v'=\sum_1^r c_i'w_i\in H$$

于是

$$H\supset\boldsymbol{Z}w_1\oplus\cdots\oplus\boldsymbol{Z}w_{r-1}\oplus\boldsymbol{Z}v'.$$

对任意 $v\in H$，减去 $v', w_1, \cdots, w_{r-1}$的适当整数倍之后，可得

$$v''=b_r w_r+b_1 w_1-\cdots+b_{r-1}w_{r-1}\in H.$$

其中$0\leqslant b_r<c_r'$，$0\leqslant b_i<1(1\leqslant i\leqslant m-1)$. 这说明 $b_r=0$，$v''\in H\cap V$，$v''=0$. 即知 $v\in \mathbf{Z}w_1\oplus\cdots\oplus\mathbf{Z}w_{r-1}\oplus\mathbf{Z}v'$. □

引理1中的 r 称为 H 的秩. 秩为 n 的 $\boldsymbol{R}^n$ 的离散子群称为**格**. 设格 $\mathscr{L}$ 的 $\mathbf{Z}$-基为 $w_1,\cdots,w_n$，则平行多面体

$$P(w_1,\cdots,w_n)=\{\sum_1^n c_i w_i\,|\,0\leqslant c_i<1\}$$

称为格 $\mathscr{L}$ 的基本区域，恰为 $\boldsymbol{R}^n/\mathscr{L}$ 的代表元集. $P(w_1,\cdots,w_n)$ 的体积(测度)$V(P(w_1,\cdots,w_n))$与 $\mathbf{Z}$-基 $w_1,\cdots,w_n$ 的选取无关，称为格 $\mathscr{L}$ 的体积，记为 $V(\mathscr{L})$.

定理1(Minkowski)　设 $\mathscr{L}$ 为 $\boldsymbol{R}^n$ 中的格，S 为 $\boldsymbol{R}^n$ 中可测子集. 若体积 $V(S)>V(\mathscr{L})$，则有 $x,y\in S$ 使$0\neq x-y\in\mathscr{L}$. (这里 $V(S)$是 S 的测度(或称体积)).

证　设　$w_1,\cdots,w_n$ 是 $\mathscr{L}$ 的 $\mathbf{Z}$—基. 于是 S 是以下形式子集的非交并集：$S\cap(h+P(w_1,\cdots,w_n))(h\in\mathscr{L})$. 故

$$V(S)=\sum_{h\in\mathscr{L}}V(S\cap(h+P)),\qquad(*)$$

因为测度 V 是平行不变量，故

$$V(S\cap(h+P))=V((-h+S)\cap P)$$

集合$(-h+S)\cap P(h\in\mathscr{L})$不能是两两非交的(否则 $V(P)\geqslant\sum_h V((-h+S)\cap P)$，与$(*)$式和 $V(P)=V(\mathscr{L})<V(S)$矛盾). 故存在 $h\neq h'$ 使$(-h+S)\cap(-h'+S)\neq\varnothing$，即有$-h+x=-h'+y$，$x$、$y\in S$. 于是 $x-y=h-h'\in\mathscr{L}$，且 $x\neq y$(因 $h\neq h'$). □

系 1 设 $\mathscr{L}$ 是 $\boldsymbol{R}^n$ 中格，S 是 $\boldsymbol{R}^n$ 的关于原点 O 对称的可测凸子集，且满足下列条件之一：

(a) $V(S)>2^nV(\mathscr{L})$,

(b) $V(S)\geqslant 2^nV(\mathscr{L})$ 且 S 是紧集.

则 S 与 $\mathscr{L}$ 有非 0 公共元.

证 (a) 令 $S'=\frac{1}{2}S$，则 $V(S')=2^{-n}V(S)>V(\mathscr{L})$. 由定理 1 知有 $y,z\in S'$ 使 $y-z\in\mathscr{L}$. 且因 S 对称且凸，故 $y-z=\frac{1}{2}(2y+(-2z))\in S$. 故 $0\neq y-z\in S\cap\mathscr{L}$.

(b) 令 $S(\varepsilon)=(1+\varepsilon)S$ $(\varepsilon>0)$，记 $\mathscr{L}_0=\mathscr{L}-\{0\}$，由(a)知 $S(\varepsilon)\cap\mathscr{L}_0$ 是非空紧集。故 $\bigcap\limits_{\varepsilon>0}S(\varepsilon)\cap\mathscr{L}_0$ 非空，设 P 为其中一点，则 $P\in S(\varepsilon)(\forall\ \varepsilon>0)$. 因 S 紧，故 $P\in S$. □

定理 2 设 K 为 n 次数域，σ: $K\longrightarrow\boldsymbol{R}^n$ 如本节开始.

(1) 设 $M\subset K$ 是秩为 n 的 $\mathbf{Z}$-模，则 $\sigma(M)$ 是 $\boldsymbol{R}^n$ 中格. 且体积

$$V(\sigma(M))=2^{-r_2}\det(\sigma_ix_j).$$

其中 $x_1,\cdots,x_n$ 是 M 的 $\mathbf{Z}$-基，$\sigma_1,\cdots,\sigma_n$ 是 K 到 $\mathbf{C}$ 的嵌入.

(2) 设 A 是 K 的整数环，I 为非 0 整理想，则 $\sigma(A)$，$\sigma(I)$ 均为 $\boldsymbol{R}^n$ 中格，且体积为

$$V(\sigma(A))=2^{-r_2}\sqrt{|D(K)|},$$

$$V(\sigma(I))=2^{-r_2}\sqrt{|D(K)|}N(I).$$

其中 $D(K)$ 为 K 的绝对判别式.

证 (1) 设$\sigma_1,\cdots,\sigma_n$是K到$\boldsymbol{C}$的嵌入映射,则

$$\sigma(x_i)=(\sigma_1(x_i),\cdots,\sigma_{r_1}(x_i),R(\sigma_{r_1+1}(x_i)),I(\sigma_{r_1+1}(x_i)),\cdots,R(\sigma_r(x_i)),I(\sigma_r(x_i))),$$

其中R,I表示实部和虚部. 于是$V(\sigma(M))=\det(\sigma(x_1),\cdots,\sigma(x_n))$(视$\sigma(x_i)$为列向量). 由$R(z)=\frac{1}{2}(z+\bar{z}),I(z)=\frac{1}{2i}(z-\bar{z})$知$V(\sigma(M))=(2i)^{-r_2}\det(\sigma_j(x_i))$. 因$\{x_j\}$是$K$的$\boldsymbol{Q}$-基,知$\det(\sigma_j(x_i))\neq 0$,故$\sigma(x_i)$在$\boldsymbol{R}^n$中线性无关,在$\boldsymbol{R}^n$中生成格$\sigma(M)$.

(2) 因A和I是秩为n的$\mathbf{Z}$-模,由(1)知$\sigma(A),\sigma(I)$为格. 若$\{x_i\}$为A的$\mathbf{Z}$-基,亦即K的整基,则$D(K)=\det(\sigma_i(x_j))^2$,即得$V(\sigma(A))$. 又$\sigma(I)$是$\sigma(A)$的子群,指数为$N(I)=\#A/I$,故$\sigma(I)$的基本区域是$\sigma(A)$的$N(I)$个基本区域之并. □

§6.3 类数与Minkowski常数

设K为$n>1$次数域,如§6.2开始,$d=D(K)$为其绝对判别式. r_1和$2r_2$为K到$\boldsymbol{C}$的实和虚嵌入个数,$N=N_{K/Q}$. 令

$$C_K=\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d|}$$

称为K的Minkowski常数.

定理1 (1) K的每个非0整理想J中必有$x\neq 0$使

$$|N(x)|\leqslant C_K N(J).$$

(2) K的每个理想类中必有理想J使

$$N(J)\leqslant C_K.$$

(3) $|d|\geqslant\frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}>1$,

从而总有素数 p 在 K 中分歧；而 $n/\log|d|$ 有上界（与 K 无关）.

(4) $h(K)$是有限正整数.

(5) (Hermite). 只有有限多个数域 $K(\subset \boldsymbol{C})$具有给定的判别式 d.

证 (1) 设 $\sigma: K \longrightarrow \boldsymbol{R}^{r_1}\times \boldsymbol{C}^{r_2}$是正则嵌入(§6.2). $\boldsymbol{R}^{r_1}\times \boldsymbol{C}^{r_2}$中满足下式的$(y_1,\cdots,y_{r_1},z_1,\cdots,z_{r_2})$全体记为 S_t:

$$|y_1|+\cdots+|y_{r_1}|+2|z_1|+\cdots+2|z_{r_2}|\leqslant t.$$

(t 为正实数). 则 S_t 是 $\boldsymbol{R}^n=\boldsymbol{R}^{r_1}\times \boldsymbol{C}^{r_2}$中关于 O 对称的紧凸集. 由积分容易算得其体积(例如见 S. Lang, *Algebraic Number Theory*, P.117)为:

$$V(S_t)=2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}t^n/n!$$

取 t 使 $V(S_t)=2^nV(\sigma(J))=2^{n-r_2}\sqrt{|d|}N(J)$, 即

$$t^n=2^{n-r_1}\pi^{-r_2}n!\ |d|^{\frac{1}{2}}N(J).$$

由上节系 1 知有非 0 元 $x\in J$ 使 $\sigma(x)\in S_t$, 故(1)由下式即得:

$$|N(x)|=|\sigma_1(x)\cdots|\sigma_{r_1}(x)|\cdot|\sigma_{r_1+1}(x)|^2\cdots|\sigma_r(x)|^2\leqslant$$
$$(|\sigma_1(x)|+\cdots+|\sigma_{r_1}(x)|+2|\sigma_{r_1+1}(x)|+\cdots+2|\sigma_r(x)|)^n/n^n$$
$$\leqslant t^n/n^n.$$

(2) 在给定理想类中任取理想 I, 令 $J=I^{-1}$, 可设 J 为整理想(否则乘以主理想). 取 $x\in J$ 满足(1), 则由 $J|(x)$知$(x)=JJ'$, J'也为整理想且与 I 属同一理想类. 于是知 $N(J)N(J')=|N(x)|\leqslant C_KN(J)$, J'满足(2).

(3) 由(2), 取 $J=(1)$知$|d|\geqslant\left(\frac{\pi}{4}\right)^n n^{2n}/n!^2$, 记此为 a_n, 则由

二项式展开知 $a_{n+1}/a_n=\frac{\pi}{4}(1+\frac{1}{n})^{2n}=\frac{\pi}{4}(1+2+\cdots)\geqslant\frac{3}{4}\pi$,因 $a_2=\frac{\pi^2}{4}$,故

$$|d|\geqslant\frac{\pi^2}{4}(\frac{3\pi}{4})^{n-2}.$$

即得(3)中不等式.取对数即得 $n/\log|d|$ 的上界. 显然有 $|d|>1$,从而总有素数 $p|d$,故 p 在 K 分歧.

(4) 注意(2)是§6.1引理1的改进,故由§6.1定理1的证明即知 $h(K)$ 有限.

(5) 由(3)知次数 n 有界. 因此不妨设 n,r_1,r_2 为固定数.

(a) 先设 $r_1\geqslant1$. 设 S 是满足下式的 $(y_1,\cdots,y_{r_1},z_1,\cdots,z_{r_2})\in\boldsymbol{R}^{r_1}\times\boldsymbol{C}^{r_2}$ 全体:

$$|y_1|\leqslant2^{n-1}(\frac{\pi}{2})^{-r_2}|d|^{\frac{1}{2}},$$

$$|y_i|\leqslant\frac{1}{2}\qquad(2\leqslant i\leqslant r_1),$$

$$|z_j|\leqslant\frac{1}{2}\qquad(1\leqslant j\leqslant r_2),$$

显然 S 是 $\boldsymbol{R}^n$ 中关于 O 对称的紧凸集,$V(S)=2^{n-r_2}|d|^{\frac{1}{2}}$. 由§6.2系1和定理2知 K 中有非0整数 x 使 $\sigma(x)\in S$,此 x 生成 K. 事实上,因 $|\sigma_i(x)|\leqslant\frac{1}{2}$ $(2\leqslant i\leqslant r_1)$,且 $|N(x)|=\prod|\sigma_i(x)|$ 为正整数,故 $|\sigma_1(x)|\geqslant1$,这说明 $\sigma_1\neq\sigma_i$(作为 $\boldsymbol{Q}(x)$ 到 $\boldsymbol{C}$ 的嵌入,$i\neq1$ 时),即知 $\boldsymbol{Q}(x)$ 为 n 次,即 $\boldsymbol{Q}(x)=K$. 由 $\sigma(x)\in S$ 知 $\sigma_i(x)(=y_i$ 或 $z_i)$ 的初等对称多项式也都是有界的,它们恰为整数 x 的首一极小多项式 $f(X)\in\boldsymbol{Z}[X]$ 的系数. 因 $f(X)$ 的次数 n 和系数均有界,故这种 $f(X)$ 的个数有限,故 x 个数有限,从而 K 的个数有限.

(*b*) 再看 $r_1=0$ 情形，令 S 是满足下式的 $(z_1,\cdots,z_{r_2})\in C^{r_2}$ 全体：

$$|I(z_1)|\leqslant 2^{n-1}(\pi/2)^{1-r_2}|d|^{\frac{1}{2}},$$

$$|R(z_1)|\leqslant\frac{1}{4},$$

$$|z_j|\leqslant\frac{1}{2}\qquad(2\leqslant j\leqslant r_2).$$

(R，I 分别表示实部和虚部)于是 S 也为以原点对称凸集，体积为 $2^{n-r_2}|d|^{\frac{1}{2}}$. 也有 K 的非 0 整数 x 使 $\sigma(x)\in S$，也可类似得到 $|\sigma_1(x)|\geqslant 1$，从而 $\sigma_1\neq\sigma_j$(作为 $Q(x)$ 到 C 的嵌入，$j\neq 1$ 时). 又由 $R(\sigma_1(x))\leqslant\frac{1}{4}$ 知 $\sigma_1(x)$ 不是实数，$\sigma_1(x)\neq\overline{\sigma_1(x)}$. 故知 $K=Q(x)$. 其余与情形(a)一样证明． □

习　题

1. 设 $K=Q(\alpha)$，α 的极小多项式为 $f(X)$，$D(K)=\mathrm{Disc}(K/Q)$，Minkowski 常数为 C_K，类数为 $h(K)$. 对以下 $f(X)$ 证明所列事实：

(1) $f(X)=X^3-X-1$，$D(K)=-23$，$C_K<2$，$h(K)=1$.

(2) $f(X)=X^3+X+1$，$D(K)=-31$，$C_K<2$，$h(K)=1$.

(3) $f(X)=X^3-2X^2+2$，$D(K)=-44$，$C_K<2$，$h(K)=1$.

(4) $f(X)=X^3-17X+31$，$D(K)=(-5)(1259)$，$h(K)=1$.

2. 设 $K=Q(\sqrt{-5})$，$L=K(\sqrt{-1})$，证明 L/K 是非分歧扩张(即 K 的任意素理想在 L 均不分歧).

§6.4 单位定理

仍设 K 为 n 次数域如 §6.2 开始，A 为其整数环，r_1 和 $2r_2$ 为 K 到 $\boldsymbol{C}$ 的实和复嵌入个数，$r=r_1+r_2$.

引理 1 若 u 是 K 的整数且范 $N(u)=N_{K/Q}(u)=\pm 1$，则 u 为 K 的单位．反之亦真．

证 由题设知 u 在 $\boldsymbol{Q}$ 上的极小多项式为 $X^n+a_{n-1}X^{n-1}+\cdots+a_1X\pm 1=0, a_i\in\boldsymbol{Z}$. 即知 $(u^{n-1}+\cdots+a_1)u=\mp 1$，故 u 是 A 中可逆元，即单位．反之显然． □

定理 1 (Dirichlet 单位定理) 数域 K 的单位群

$$U(K)\cong W\times\boldsymbol{Z}^{r-1},$$

其中 W 是有限循环群(从而为 K 中单位根全体组成的群，偶数阶)，$r=r_1+r_2$. 也就是说，K 中单位恰为全体

$$u=w\eta_1^{n_1}\eta_2^{n_2}\cdots\eta_{r-1}^{n_{r-1}}\qquad(n_i\in\boldsymbol{Z}).$$

其中 w 是单位根，η_i 生成无限循环群. ($\eta_1,\cdots,\eta_{r-1}$ 称为 K 的一个基本单位系).

证 为了将乘法群 $U=U(K)$ 对应到 $\boldsymbol{R}^r$ 的加法子群，必须取对数. 设嵌入 $\sigma_1,\cdots,\sigma_r$ 如 §6.2 开始，令

$$l: U(K)\longrightarrow\boldsymbol{R}^r,$$

$$x\longmapsto(\log|\sigma_1(x)|,\cdots,\log|\sigma_r(x)|),$$

l 称作**对数嵌入**，显然是群同态. 我们先证明：$l(U)$ 是离散子

群. 为此设 S 是 $\boldsymbol{R}^r$ 的一个有界子集，$S' = \{x \in U \mid l(x) \in S\}$. 因 S 有界故存在实数 $c > 1$ 使对 $x \in S'$ 有 $c^{-1} \leqslant |\sigma_i(x)| \leqslant c$ $(1 \leqslant i \leqslant r)$. 故 $\sigma_i(x)$ 的初等对称多项式也有界，它们恰为 x 在 $\boldsymbol{Q}$ 上的首一极小多项式 $f(X) \in \boldsymbol{Z}[X]$ 的整数系数，故 $f(X)$，从而 x 的个数有限，故 S' 是有限集，$l(U)$ 是 $\boldsymbol{R}^r$ 的离散子群. 由 S' 的有限性可知，l 在 U 上限制 l' 的核 W 是有限群. 因此 W 是有限循环群(由下述引理 2)，是 ω 次复单位根全体(ω 为某整数). W 恰为 K 中的单位根全体，因若 $\alpha^m = 1$ 则 α 是整数且 $|\sigma_i(\alpha)|^m = 1$，故 $|\sigma_i(\alpha)| = 1(1 \leqslant i \leqslant r)$，即知 $\alpha \in \ker(l') = W$. 因 W 含 2 阶子群$\{\pm 1\}$，故阶为偶数.

由于 $l(U)$ 是 $\boldsymbol{R}^r$ 的离散子群，故由 §2 引理 1 知 $U/W \cong l(U) \cong \boldsymbol{Z}^s$，即 $U \cong W \times \boldsymbol{Z}^s$. 以下证明 $s = r - 1$.

首先易知 $s \leqslant r - 1$. 事实上，对 $x \in U$，$\sigma_i(x)$ 之间有关系：

$$\pm 1 = N(x) = \sigma_1(x) \cdots \sigma_n(x)$$
$$= \sigma_1(x) \cdots \sigma_{r_1}(x) |\sigma_{r_1+1}(x)|^2 \cdots |\sigma_r(x)|^2,$$

故

$$0 = \log|\sigma_1(x)| + \cdots + \log|\sigma_{r_1}(x)| + \cdots + 2\log|\sigma_r(x)|,$$

即 $l(x)$ 属于 $\boldsymbol{R}^r$ 的 $r - 1$ 维超平面

$$\mathscr{H}: 0 = y_1 + \cdots + y_r.$$

即 $l(U) \subset \mathscr{H}$，从而知 $l(U)$ 的秩 $s \leqslant r - 1$.

再证 $s \geqslant r - 1$，只需举出 $l(U)$ 中有 $r - 1$ 个线性无关的向量. 为此只需证明，对 $\mathscr{H}$ 上的每个非 0 线性函数 f，存在 $u \in U$ 使 $f(l(u)) \neq 0$. (因为 m 维空间上的线性函数构成一个 m 维空间). 对 $y = (y_1, \cdots, y_r) \in \mathscr{H}$，$f(y)$ 必形如

$$f(y) = c_1 y_1 + \cdots + c_{r-1} y_{r-1}, \qquad c_i \in \boldsymbol{R} \tag{1}$$

这是因为 $y_r = -y_1 - \cdots - y_{r-1}$.

(i) 对任意 $\lambda = (\lambda_1, \cdots, \lambda_{r-1}) \in \boldsymbol{R}^{r-1}$，先求有良好性质的 x_λ

$\in K$. 固定实数 $\alpha > 2^{n}(1/2\pi)^{r_2}|d|^{\frac{1}{2}}$，取 $\lambda_r > 0$（并记 $\lambda_{r+1} = \lambda_{r_1+1}, \cdots, \lambda_{r+r_2} = \lambda_{r_1-r_2}$）使 $\lambda_1\cdots\lambda_{r_1}\cdots\lambda_r\cdots\lambda_n = \alpha$.

设满足下式的 $(y_1, \cdots, y_{r_1}, z_1, \cdots, z_{r_2}) \in \boldsymbol{R}^{r_1} \times \boldsymbol{C}^{r_2}$ 全体为 S：

$$|y_i| \leqslant \lambda_i, \ |z_j| \leqslant \lambda_j$$

则 S 是关于 0 对称的有界凸集，体积

$$V(S) = \prod_{i=1}^{r_1} 2\lambda_i \prod_{j=r_1+1}^{r} \pi\lambda_j^2 = 2^{r_1}\pi^{r_2}\alpha > 2^{n-r_2}|d|^{\frac{1}{2}}.$$

故存在 K 的整数 x_λ 使 $\sigma(x_\lambda) \in S$（§6. 2 定理 2 及系 1）. 这意味着 $|\sigma_i(x_\lambda)| \leqslant \lambda_i (1 \leqslant i \leqslant n)$. 因为 x_λ 是整数，故

$$1 \leqslant |N(x_\lambda)| = |\sigma_1(x_\lambda)\cdots\sigma_n(x_\lambda)| \leqslant \lambda_1\cdots\lambda_n = \alpha.$$

$$|\sigma_i(x_\lambda)| \geqslant \prod_{j\neq i} \sigma_j(x_\lambda)^{-1} \geqslant \lambda_i/\alpha$$

故

$$\lambda_i/\alpha \leqslant |\sigma_i(x_\lambda)| \leqslant \lambda_i$$

即

$$0 \leqslant \log\lambda_i - \log|\sigma_i(x_\lambda)| \leqslant \log\alpha. \ (1 \leqslant i \leqslant n), \qquad (2)$$

注意 $(\log|\sigma_i(x_\lambda)|)$ 是 $l(x_\lambda)$ 的坐标，故由(1) 式知

$$|f(l(x_\lambda) - \sum_{i=1}^{r-1} c_i\log\lambda_i| \leqslant (\sum_{1}^{r-1}|c_i|)\log\alpha, \qquad (3)$$

(ii) 再求特殊的 x_λ 得出 u. 设 β 是大于(3) 式右边的正整数. 对每个正整数 h，取 $\lambda(h) = (\lambda_{h_1}, \cdots, \lambda_{h_{(r-1)}}) \in \boldsymbol{R}^{r-1}$ 使 $\sum_{i=1}^{r-1} c_i\log\lambda_{h_i} = 2\beta h$，由(i) 得出 $x_{\lambda(h)}$，记为 x_h. 由(3) 式有

$$|f(l(x_h)) - 2\beta h| < \beta,$$

$$(2h-1)\beta < f(l(x_h)) < (2h+1)\beta \qquad (4)$$

这说明 $f(l(x_h))$ 两两不同（对不同的 h）. 而由于 $|N(x_h)| \leqslant \alpha$，

故主理想(x_h)只有有限多个，故存在整数 $h \neq k$ 使得

$$(x_h) = (x_k),$$

从而 $u = x_h/x_k$ 为单位，故

$$\begin{aligned} f(l(u)) &= f(l(x_h) - l(x_k)) \\ &= f(l(x_h)) - f(l(x_k)) \neq 0. \end{aligned}$$

□

系 1 $u \in U(K)$ 为单位根当且仅当 $|u|_{\infty_i} = 1 (1 \leqslant i \leqslant r)$，这里 $\infty_1, \cdots, \infty_r$ 是 K 的 r 个无限素除子.

证 由上述证明可知单位根群 $W = \ker(l')$，即知 u 为单位当且仅当 $\log|\sigma_i(u)| = 0$，即 $|\sigma_i(u)| = 1$，亦即 $|u|_{\infty_i} = 1$.

引理 2 (1) 设G是有限 Abel 群，则存在 $x_0 \in G$，使 x_0 的阶等于 G 中所有元素 x 的阶的最小公倍数.

(2) 域 K 的乘法有限子群 W 必为循环群.

证 (1) 将 G 的运算记为加法，由 Abel 群(或主理想环 $\mathbf{Z}$ 上的模)基本定理知 $G \cong \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}$，$a_i | a_j$(当 $i < j$)，a_i 是正整数. 于是 $x = (0, \cdots, 0, \bar{1})$ 的阶为 a_n，显然 x 即所欲求.

(2) 由 (1) 知存在 n 阶元 $x_0 \in W$，使 $x^n = 1$(对所有 $x \in W$). 由于 $X^n - 1$ 在域 K 中最多有 n 个根，故 W 至多有 n 个元素. 但因 x_0 的阶是 n，故 $1, x_0, \cdots, x_0^{n-1}$ 必是 n 个不同元素，即知 $W = \{1, x_0, \cdots, x_0^{n-1}\}$. □

我们可以将单位和单位定理稍作推广，这在类域论等理论中十分重要. 以 S_∞ 表示 M_K(K 的素除子集) 中无限素除子全

体. 设 S 是含 S_∞ 的 M_K 的有限子集，记 $s = \# S$. 比如

$$S = \{\infty_1, \cdots, \infty_r, v_{r+1}, \cdots, v_s\},$$

$u \in K$ 称为 **S- 单位**是指

$$|u|_v = 1 \qquad (对所有素除子 v \notin S).$$

S-单位全体记为U_S或$U_S(K)$，是乘法群. 显然S_∞-单位就是普通单位. 定义 $U_S(K)$ 到 $\boldsymbol{R}^s$ 的嵌入为

l_s: $x \longmapsto (\log\|x\|_1, \cdots, \log\|x\|_s)$，其中 $\|\ \|_i$ 是 $v_i \in M_k$ 的对 K 标准化的赋值，即当 v_i 是 $\wp_i$—adic 赋值时，对素元 $\pi_i \in \wp_i - \wp_i^2$ 有

$$\|\pi\|_i = (N\wp_i)^{-1} = p^{-f_i} = |\pi|_i^{-e_if_i};$$

当 $K_{v_i} = \boldsymbol{C}$时有 $\|a\|_i = |a|^2$; 当$K_{v_i} = \boldsymbol{R}$时有 $\|a\|_i = |a|$. 我们需要

引理 3 (乘积公式). 对任意非零的 $\alpha \in K$ 有

$$\prod_{v \in M_K} \|\alpha\|_v = 1.$$

证 我们已知乘积公式对$K = \boldsymbol{Q}$成立. 于是由第 4 章 §8 系 4 知

$$1 = \prod_{v_0 \in M_Q} |N_{K/Q}(\alpha)|_{v_0} = \prod_{v_0 \in M_Q} \prod_{v | v_0} |\alpha_v|^{n_v}$$

$$= \prod_{v \in M_K} |\alpha|_v^{n_v} = \prod_{v \in M_K} \|\alpha\|_v. \qquad \square$$

现设 $\alpha \in A$ 是 K 的整数，若 $\alpha \in U_S(K)$，即当 $v \notin S$ 时 $\|\alpha\|_v = |\alpha|_v^{n_v} = 1$，则由乘积公式知

$$\prod_{v \in S} \|\alpha\|_v = 1. \qquad (5)$$

反之，若(5) 式成立，则由乘积公式可知$\prod_{v \notin S} \|\alpha\|_v = 1$，再由

$\|\alpha\|_v \geqslant 1$(因 $\alpha \in A$) 可知 $\|\alpha\|_v = 1$ 对 $v \notin S$ 成立，即知 $\alpha \in U_S(K)$. 故整数 α 是 S- 单位当且仅当(5) 式成立. 引理 1 是此论断的特殊情形.

由乘积公式或(5) 式可知，$l_S(U_S)$ 在如下 $s-1$ 维超平面上：

$$\mathscr{H}_S:\ y_1 + \cdots + y_s = 0.$$

于是与定理 1 的证明类似可以证明：

定理 2 （单位定理）数域 K 的 S- 单位群

$$U_S(K) \cong W \times \mathbf{Z}^{s-1}$$

其中 W 是有限循环群(即 K 中单位根全体)，$s = \# S$.

当 K 为 $\boldsymbol{F}_q(X)$ 的有限扩张时，定理 2 也成立，证明也完全类似(这里 $\boldsymbol{F}_q(X)$ 为有限域 $\boldsymbol{F}_q$ 上的有理式形式域，也称有理函数域). 我们回忆，$k = \boldsymbol{F}_q(X)$ 的素除子集为$\{\infty, p(X) \mid p(X)$ 为不可约多项式$\}$，其中 $p(X)$ 对应 $p(X)$--adic 赋值. ∞ 对应 $\dfrac{1}{X}$ — adic 赋值. K 的素除子由 k 的素除子延拓而得. 其中由 ∞ 延拓的 K 的素除子集记为 S_∞. 仍取 S 为含 S_∞ 的有限集合.

习　　题

1. 设 K 为数域，$\eta_1, \cdots, \eta_{r-1}$ 是其基本单位. $r-1$ 阶行列式

$$\det(\log \|\sigma_i(\eta_j)\|) \quad (1 \leqslant i, j \leqslant r-1)$$

的绝对值称为 K 的**正规子**(regulator)，记为 $R(K)$. 证明 $R(K) > 0$ 且不依赖于基本单位的选取. 如果 $\eta_1, \cdots, \eta_{r-1}$ 不是基本单位，上述行列式又当如何？

第七章　二次域与分圆域

§7.1　二次域的单位群

先设 K 是虚二次域. 于是 $r_1 = 0$, $2r_2 = 2$, $r_1 + r_2 - 1 = 0$. 由上节单位定理可知, K 的单位群 $U(K) = W$, 即单位根形成的循环群. 注意 W 含二阶子群 $\{1, -1\}$, 故必为偶数阶. 设 $W = \langle \zeta_m \rangle$ 由 m 次本原单位根生成, 可设 m 为偶数. 于是

$$K \supset \boldsymbol{Q}(\zeta_m).$$

这说明 $\boldsymbol{Q}(\zeta_m)$ 只能是虚二次域或 $\boldsymbol{Q}$. 特别知 $\boldsymbol{Q}(\zeta_m)$ 的次数

$$\varphi(m) = 2 \text{ 或 } 1.$$

设　$m = 2^{a_0} p_1^{a_1} \cdots p_s^{a_s}$, 则

$$\varphi(m) = 2^{a_0 - 1} p_1^{a_1 - 1}(p_1 - 1) \cdots p_s^{a_s - 1}(p_s - 1).$$

故只能有如下的情形: $m = 2, 2^2, 2 \cdot 3$.

当 $m = 2$ 时, $W = \{1, -1\}$, $\boldsymbol{Q}(\zeta_m) = \boldsymbol{Q}$.

当 $m = 4$ 时, $W = \{1, -1, i, -i\} = \langle i \rangle$, $\boldsymbol{Q}(\zeta_m) = \boldsymbol{Q}(\sqrt{-1})$, 其中 $i = \sqrt{-1}$.

当 $m = 6$ 时, $W = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$, $\boldsymbol{Q}(\zeta_m) = \boldsymbol{Q}(\sqrt{-3})$, 其中 $\rho = (1 + \sqrt{-3})/2$. 故得

命题 1 虚二次域 K 的单位群

$$U(K)=\begin{cases}\text{四阶群}\langle i\rangle, & \text{当 } K=\boldsymbol{Q}(\sqrt{-1});\\ \text{六阶群}\langle \rho\rangle, & \text{当 } K=\boldsymbol{Q}(\sqrt{-3});\\ \text{二阶群}\langle -1\rangle, & \text{其余情形.}\end{cases}$$

再设

$$K=\boldsymbol{Q}(\sqrt{d})$$

为实二次域，d 为无平方因子有理整数. 因复平面上单位圆与实轴只两个交点，故 $W=\{1,-1\}$. $r_1=2$，$r_2=0$，故 $r_1+r_2-1=1$. 于是 K 的单位群

$$U(K)=\{\pm 1\}\times\varepsilon^{Z}$$

其中 ε 生成无限循环群 $\langle\varepsilon\rangle=\varepsilon^{Z}$. 显然 $\pm\varepsilon$ 和 $\pm\varepsilon^{-1}$ 也都生成无限循环群，我们常取其中唯一一个大于1的记为 ε，称为 K 的**基本单位**.

设 $\alpha=a+b\sqrt{d}\,(a,b\in\boldsymbol{Q})$ 是 K 的单位，则 $\pm\alpha$，$\pm\alpha^{-1}$ 均为单位. 由于 $N(\alpha)=(a+b\sqrt{d})(a-b\sqrt{d})=\pm 1$，故上述四个数就是 $\pm a\pm b\sqrt{d}$，四者中只有一个大于 1，它也是四者中最大的. 因此 K 的大于 1 的单位均形如 $a+b\sqrt{d}\,(a>0,b>0)$.

(1) 先设 $d\equiv 2$ 或 $3(\bmod 4)$. 此时 K 的整数环为 $\boldsymbol{Z}+\boldsymbol{Z}\sqrt{d}$. 整数 $\alpha=x+y\sqrt{d}\,(x,y\in\boldsymbol{Z})$ 为单位当且仅当 $N(\alpha)=\pm 1$，即

$$x^2-dy^2=\pm 1 \tag{1}$$

这称为 Pell 方程. 由单位定理可知，若 $\varepsilon=a_1+b_1\sqrt{d}$ 是 K 的基本单位($a_1>0$，$b_1>0$)，则 $(a_1+b_1\sqrt{d})^n=a_n+b_n\sqrt{d}$ 为大于 1 的单位，(a_n,b_n) 是 Pell 方程的自然数解. (当然($\pm a_n$,

$\pm b_n$) 均为解). 此时也称 $a_n + b_n\sqrt{d}$ 和 $\pm a_n \pm b_n\sqrt{d}$ 为 Pell 方程的解. 易知 $b_{n+1} = a_1 b_n + b_1 a_n$, 故序列 $\{b_n\}$ 是严格递增的. 因此依次考查 $b = 1, 2, 3, \cdots$, 当第一次发现 $db^2 \pm 1$ 为平方数 a^2 时, $a + b\sqrt{d}$ 就是基本单位了. 如 $d = 2$ 时 $\varepsilon = 1 + \sqrt{2}$, $d = 3$ 时, $\varepsilon = 2 + \sqrt{3}$, $d = 6$ 则 $\varepsilon = 5 + 2\sqrt{6}$, $d = 7$ 则 $\varepsilon = 8 + 3\sqrt{7}$ 等.

如果 $N(\varepsilon) = 1$, 则 $x^2 - dy^2 = -1$ 无解, $\pm\varepsilon^n$ 均为 $x^2 - dy^2 = 1$ 的解. 如果 $N(\varepsilon) = -1$, 则 $\pm\varepsilon^{2n+1}$ 为 $x^2 - dy^2 = -1$ 的解, $\pm\varepsilon^{2n}$ 为 $x^2 - dy^2 = 1$ 的解($n \in \mathbf{Z}$).

(2) 设 $d \equiv 1 (\mathrm{mod} 4)$. K 的整数为 $\alpha = (a + b\sqrt{d})/2$, $a \equiv b(\mathrm{mod} 2)$, $a, b \in \mathbf{Z}$. 若 α 为单位, 则 $\pm 1 = N(\alpha) = (a^2 - b^2 d)/4$, 故 (a, b) 满足方程

$$x^2 - dy^2 = \pm 4 \tag{2}$$

这也称为 Pell 方程. 反之, 若 (a, b) 是方程(2) 的整数解, 则 $\alpha = (a + b\sqrt{d})/2$ 必为 K 中整数(因 $\alpha^2 - a\alpha \pm 1 = 0$), 且范为 ± 1, 故 α 必为单位. 设 K 的基本单位为 $\varepsilon = (a_1 + b_1\sqrt{d})/2$, 则由

$$\varepsilon^n = \left(\frac{a_1 + b_1\sqrt{d}}{2}\right)^n = \frac{a_n + b_n\sqrt{d}}{2}$$

给出 Pell 方程(2) 的全部自然数解(a_n, b_n)(此时也称$(a_n + b_n\sqrt{d})/2$ 为 Pell 方程一解). 也可象(1) 中那样依次考查 $b = 1, 2, 3, \cdots$, 第一个平方数 $db^2 \pm 4 = a^2$ 即给出基本单位$(a + b\sqrt{d})/2$.

子环 $A_0 = \mathbf{Z}[\sqrt{d}]$ 中的单位 $a + b\sqrt{d}$ 对应着方程

$$x^2 - dy^2 = \pm 1 \tag{3}$$

的解, 这些单位形成 $U(K)$ 的子群 $U_0(K)$. 如果基本单位 $\varepsilon = a$

$+b\sqrt{d}\in U_0(K)$，自然$U(K)=U_0(K)$(例如$d=17$时). 如果基本单位$\varepsilon=(a+b\sqrt{d})/2$，$a$和$b$均奇数，则$\varepsilon\notin U_0(K)$. 但易知$\varepsilon^3\in U_0(K)$. 事实上，$8\varepsilon^3=a(a^2+3b^2d)+b(3a^2+b^2d)\sqrt{d}$. 而

$$a^2+3b^2d=(b^2d\pm 4)+3b^2d=4b^2d\pm 4\equiv 0(\mathrm{mod}8),$$

$$3a^2+b^2d=3(b^2d\pm 4)+b^2d=4b^2d\pm 12\equiv 0(\mathrm{mod}8).$$

显然$\varepsilon^2\notin U_0(K)$(否则$\varepsilon=\varepsilon^3/\varepsilon^2\in U_0(K)$)，故此时$U_0(K)=\{\pm 1\}\times\langle\varepsilon^3\rangle=\{\pm 1\}\times\varepsilon^{3Z}$. 例如$d=5$时，$\varepsilon=(1\pm\sqrt{5})/2$，$\varepsilon^2=(3+\sqrt{5})/2$，$\varepsilon^3=2+\sqrt{5}$.

命题 2 设实二次域$Q(\sqrt{d})$的基本单位为ε，则

(i) 若d有素因子$q\equiv 3(\mathrm{mod}4)$，则$N(\varepsilon)=1$.

(ii) d为素数$p\equiv 1(\mathrm{mod}4)\Leftrightarrow N(\varepsilon)=-1$.

(iii) 整数m可表为两整数的平方之和$\Leftrightarrow$若m有素因子$q\equiv 3(\mathrm{mod}4)$，则$q^{2s}\parallel m$ $(s\in\mathbf{Z})$.

证 (i) 若$-1=N(\varepsilon)=a^2-b^2d\equiv a^2(\mathrm{mod}q)$说明$(-1/q)=1$，即$-1$是模$q$平方剩余，故$q\equiv 1(\mathrm{mod}4)$，矛盾.(注意 (i) 的逆命题不真，例如$d=34$时，$N(\varepsilon)=N(35+6\sqrt{34})=1$).

(iii) 先证素数$p\equiv 1(\mathrm{mod}4)$可表为两整数平方和. 事实上由$(-1/p)=1$知p在$\mathbf{Q}(i)=Q(\sqrt{-1})$中分裂，且$Q(i)$的整数环$B=\mathbf{Z}[i]$为主理想环(实际上易知$\mathbf{Z}[i]$是欧几里得环)，故

$$(p)=\wp\overline{\wp}=(a+bi)(a-bi)=(a^2+b^2),$$

即知$p=a^2+b^2$，而$p_1\cdots p_s=\wp_1\overline{\wp}_1\cdots\wp_s\overline{\wp}_s=((a_1+$

$b_1i)\cdots(a_s+b_si))((a_1-b_1i)\cdots(a_s-b_si))=(s+ti)(s-ti)=(s^2+t^2)$，这就证明了充分性.

现设 $m=a^2+b^2=(a+bi)(a-bi)$，a，b 为正整数. 若 m 有素因子 $q\equiv 3(\mathrm{mod}4)$，由 $(-1/q)=-1$ 知 (q) 为 $\boldsymbol{Z}[i]$ 的素理想，故若 $(q)^s\parallel(a+bi)$ 则 $(q)^s\mid(a-bi)$，从而 $q^{2s}\parallel m$.

(ii) 设 $p=a^2+b^2=(a+bi)(a-bi)$，a，b 为互素正整数. 故存在 s，$t\in\boldsymbol{Z}$ 使 $sa+tb=1$，即知虚部 $I((a+bi)(t+si))=1$. 设 $\sqrt{t+si}=c+ei$，$y=c^2+e^2$，则

$$
\begin{aligned}
y^2&=(c^2+e^2)^2=((c+ei)(c-ei))^2\\
&=(c+ei)^2(c-ei)^2=(t+si)(t-si),\\
py^2&=((a+bi)(t+si))((a-bi)(t-si))\\
&=(x+i)(x-i)=x^2+1,
\end{aligned}
$$

故

$$x^2-py^2=-1,$$

其中 $x=at-bs\in\boldsymbol{Z}$，故 $y\in\boldsymbol{Z}$，这说明 $N(\varepsilon)=-1$. □

7.1.1 二次域的单位与连分数

实二次域 $K=\boldsymbol{Q}(\sqrt{d})(d>5)$ 的基本单位 ε，可由 $\sqrt{d}$ 的简单连分数展开求出. 这也是解 Pell 方程

$$x^2-dy^2=c\qquad(c=\pm1,\pm4)$$

的有效方法. 对实数 α，以 $[\alpha]$ 记其整数部分.

展 $\sqrt{d}$ 为简单连分数求 ε 和解 Pell 方程步骤如下：

令 $[\sqrt{d}]=a_0$，　记 $\beta_1=(\sqrt{d}-a_0)^{-1}=\dfrac{\sqrt{d}+P_1}{Q_1}$　$(P_1,Q_1\in\boldsymbol{Z})$；

令 $[\beta_1]=a_1$，　记 $\beta_2=(\beta_1-a_1)^{-1}=\dfrac{\sqrt{d}+P_2}{Q_2}$　$(P_2,Q_2\in\boldsymbol{Z})$；

…………………………………………

令$[\beta_{n-1}]=a_{n-1}$，记 $\beta_n=(\beta_{n-1}-a_{n-1})^{-1}=\dfrac{\sqrt{d}+P_n}{Q_n}(P_n,Q_n\in \mathbf{Z})$.

直到在序列

$$Q=(Q_0,Q_1,Q_2,\cdots)$$

中，第一次见到某 $Q_n=\pm 1$ 或 ± 4（确切言之，设 $Q_n=(-1)^n c$)（常记 $Q_0=1$)，则

$$\varepsilon=p_{n-1}+q_{n-1}\sqrt{d}$$

即为 $\mathbf{Q}(\sqrt{d})$ 的基本单位（确切言之，ε 是 $x^2-dy^2=c$ 的基本解)，其中 p_{n-1}，q_{n-1} 由下式递归给出：

$$p_i=a_ip_{i-1}+p_{i-2},\quad p_{-1}=1,\quad p_0=a_0;$$

$$q_i=a_iq_{i-1}+q_{i-2},\quad q_{-1}=0,\quad q_0=1.$$

上述步骤也得出 $\sqrt{d}$ 的连分数展开为

$$\sqrt{d}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cdots}}=[a_0,a_1,a_2,\cdots].$$

例如，对 $d=\sqrt{19}$ 有

$$\sqrt{19}=[a_0,a_1,\cdots]=[4,\overline{2,1,3,1,2,8}],$$

$$Q=(Q_0,Q_1,\cdots)=(1,\overline{3,5,2,5,3,1}).$$

（其中上划线部分表示循环，例如$\overline{1,2,3}=1,2,3,1,2,3,1,2,3,\cdots$). 故首次有 $Q_6=1$，易知 $p_5=170$，$q_5=39$，即得 $\mathbf{Q}(\sqrt{19})$ 的基本单位为 $\varepsilon=170+39\sqrt{19}$.

连分数的理论在许多初等数论书中均有（例如可见华罗庚的《数论导引》). 易证明对每个 Q_n（称为连分数第 n 个完全分母)，总有

$$p_{n-1}^2 - dq_{n-1}^2 = (-1)^n Q_n.$$

而且当 $|c| < \sqrt{d}$ 时，Pell 方程 $x^2 - dy^2 = c$ 有互素整数解 x，y 当且仅当 $c = (-1)^n Q_n$ 对某 n 成立. 我们在[Zh10]中将此结果发展到适合 $|c| \geqslant \sqrt{d}$ 的情形(用半单连分数).

还可以证明，$\sqrt{d}$ 的简单连分数展开总是周期性的，即

$$\sqrt{d} = [a_0, \overline{a_1, \cdots, a_{k-1}, 2a_0}],$$

$$Q = (1, \overline{Q_1, \cdots, Q_{k-1}, 1}),$$

而且 $\quad a_i = a_{k-i}, Q_i = Q_{k-i} \quad (1 \leqslant i \leqslant k-1)$.

有些类型的实二次域的基本单位可统一求出. 例如设

$$d = s^2 + r, \qquad r \mid 4s,$$

其中 $s, r \in \mathbf{Z}$, $s > 0$, 且 $-s < r < 4(s+1)/3$, $d > 5$, 则 $\boldsymbol{Q}(\sqrt{d})$ 的基本单位

$$\varepsilon = \begin{cases} s + \sqrt{d}, & 若 r = \pm 1, \\ (s + \sqrt{d})/2, & 若 r = \pm 4, \\ (s + \sqrt{d})^2/r, & 若 |r| \neq 1 或 4. \end{cases}$$

这可由 $\sqrt{d}$ 的连分数展开得出，留给读者作为练习.

习　题

1. 设 $K = \boldsymbol{Q}(\sqrt{d_1}, \cdots, \sqrt{d_n})$ 为 2^n 次数域. 试证明 K 中单位根群 $\langle\zeta_\omega\rangle$ 能且只能有六种情形(ζ_ω 为 ω 次本原单位根)：

$$\omega = 2, 4, 8, 6, 12, 24.$$

2. 试证明 $\sin\theta^\circ$ 和 $\cos\theta^\circ$ 均可表为形式

$$\sum_i a_i \sqrt{d_i} \qquad (a_i, d_i \in \boldsymbol{Q})$$

的充分必要条件为 θ 是 15 的整数倍(提示：由习题 1).

§ 7.2 欧几里得域

设二次域

$$K = \boldsymbol{Q}(\sqrt{d}),$$

其中 d 为无平方因子有理整数. 以 $A = O_K$ 记其整数环, $H(K) = H(d)$ 记其理想类群, $h(K) = h(d)$ 记其理想类数.

先探讨 $A = O_K$ 何时是欧几里得环. 按第二章定义, 若有映射 $\varphi: A \longrightarrow \boldsymbol{N}$ 使对任意 $\alpha, \beta \in A$, $\beta \neq 0$ 总有 $\alpha = \beta q + r (q, r \in A)$ 满足条件 $\varphi(r) < \varphi(\beta)$, 则 A 称为欧几里得环, φ 称为欧几里得映射. (此时也称域 K 为欧几里得域).

古典的讨论总是假定 φ 为范映射. 我们也先如此, 暂时先设 $\varphi(\alpha) = |N(\alpha)| = |N_{K/Q}(\alpha)|$. 若对 $\alpha, \beta \in A$, $\beta \neq 0$ 有

$$\alpha = q\beta + r,$$

则欧几里得环的条件 $|N(r)| < |N(\beta)|$ 相当于 $|N((\alpha/\beta) - q)| < 1$. 记 $\theta = \alpha/\beta \in A$. 先设 $d \equiv 2$ 或 $3 \pmod 4$, 记 $\theta = a + b\sqrt{d}$, $q = x + y\sqrt{d}$ $(a, b \in \boldsymbol{Q},\ x, y \in \boldsymbol{Z})$. 令 $c = a - x$, $s = b - y$. 于是条件化为

$$|N(\theta - q)| = |N(r + s\sqrt{d})| = |c^2 - ds^2| < 1. \quad (*)$$

显然可选取 x, y 使 $|c| \leqslant \frac{1}{2}$, $|s| \leqslant \frac{1}{2}$, 则 $(*)$ 式对 $d = -2, -1, 2, 3$ 满足, 相应的域为欧几里得域.

再设 $d \equiv 1 \pmod 4$. 记 $\theta = a + b(1 + \sqrt{d})/2$, $q = x + y(1 + \sqrt{d})/2$, $c = a - x$, $s = b - y$ $(a, b \in \boldsymbol{Q},\ x, y \in \boldsymbol{Z})$. 条件 $|N(r)| < |N(\beta)|$ 变为

$$\begin{aligned} |N(\theta - q)| &= |N(c + s(1 + \sqrt{d})/2)| \\ &= |(c + s/2)^2 - d(s/2)^2| < 1. \qquad (**) \end{aligned}$$

显然可取 y 使 $|s| \leqslant \frac{1}{2}$，再取 x 使

$$|c + s/2| = |a + b/2 - y/2 - x| \leqslant \frac{1}{2}.$$

于是知道 $d = -11, -7, -3, 5, 13$ 时 K 为欧几里得域，而且显然(∗∗)对其余的负的 d 不再满足.

定理 1 (1) 当 $d = -1, -2, -3, -7, -11$ 时，$K = \boldsymbol{Q}(\sqrt{d})$ 为欧几里得域(且范映射为欧几里得映射). 其余虚二次域均非欧几里得域(对任何可能的欧几里得映射).

(2) 当 $d = 2, 3, 5, 13$ 时，$\boldsymbol{Q}(\sqrt{d})$ 为欧几里得域(且范映射为欧几里得映射).

引理 1 设 A 为环且是可数集. 记 $A_0 = \{0\}$. 对正整数 $n \in N$，归纳定义 $A'_n = \bigcup_{m<n} A_m$，$A_n = \{0\} \cup \{b \in A \mid A'_n \to A/Ab$ 为满射$\}$. 则 A 为欧几里得环当且仅当递升序列 A_n 穷尽 A.

证 $A'_n \to A/Ab$ 为满射的意思是，A/Ab 的每个剩余类中均有 A'_n 的元素. 上述引理对不可数的 A 也成立，但 N 应代之以比 A 基数大的良序集 W. 证明见 P. Samuel: *About Euclidean Rings*, *J. of Number Theory*, 19(1971), 202—301.

定理 1 的证明 只需再证其余虚二次域 K 均非欧几里得域，故 K 的单位仅为 ± 1. 由引理 1，记 $A_0 = \{0\}$，$A'_1 = \{0\}$. $\{0\} \to A/Ab$ 为满射意味着 $A/Ab = 0$，即 b 是单位，$b = \pm 1$. 故 $A_1 = \{0, 1, -1\}$. 于是 $A'_2 = \{0, 1, -1\}$. $A'_2 \to A/Ab$ 为满射意味着 $\# A/Ab \leqslant 3$，即 $|N(b)| = 1, 2, 3$. 若 $|N(b)| = 1$,

则 b 为单位，$b=\pm 1$.

(1) 当 $d\equiv 2$ 或 $3(\mathrm{mod}4)$ 时，$|N(b)|=2$ 或 3 意味着 $x^2+|d|y^2=2$ 或 3 有整数解，易知 $|d|\leqslant 3$.

(2) 当 $d\equiv 1(\mathrm{mod}4)$ 时，$x^2+|d|y^2=8$ 或 12 应有整数解，易知 $|d|\leqslant 12$，即 $d=-7,-11$.

对其余的 d 值，不可能有 b 使 $|N(b)|=2$ 或 3. 故 $A_2=A_1$，即序列 $\{A_n\}$ 在 $n=1$ 时停止上升，$A_1=\{0,1,-1\}$ 未穷尽 A，故 A 不是欧几里得环(对任何可能的欧几里得映射 φ). □

注记 对实二次域 $\boldsymbol{Q}(\sqrt{d})$，已证明有且只有 16 个域对范映射是欧几里得域：$d=2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73$. 是否还有别的域对别的欧几里得映射为欧几里得域的问题尚未解决.

§7.3 二次域的类数

仍设 $K=\boldsymbol{Q}(\sqrt{d})$ 为二次域，类数为 $h=h(K)=h(d)=h(D)$，D 为 K 的判别式. 对二次域 K，Minkowski 常数为

$$C_K=\begin{cases}\dfrac{2}{\pi}\sqrt{|D|}, & \text{当 } K \text{ 为虚二次域；}\\[2ex] \dfrac{1}{2}\sqrt{|D|}, & \text{当 } K \text{ 为实二次域.}\end{cases}$$

于是每个理想类中必有整理想 J 使 $N(J)\leqslant C_K$.

先看虚二次域. 若 $|D|\leqslant 9$，则 $C_K<2$，故只能 $h(K)=1$. 若 $D=-11,-19$，则 $C_K<3$，故每类中含 J 使 $N(J)=2$ 或 1，由 $-11\equiv-19\equiv 5(\mathrm{mod}8)$ 知 2 惯性，故 J 只能为 2，由 $N(2)=4$ 知不可，故此时也有 $h(K)=1$.

定理 1 (Gauss-Baker-stark) 恰有 9 个虚二次域 $K = \boldsymbol{Q}(\sqrt{d})$ 的类数为 $h(d) = 1$，即

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

证明 我们只对 $|D| < 520$ 证明，其余见注记 1(1). 首先注意对 $\alpha = (x + y\sqrt{D})/2 \in A$, $x, y \in \boldsymbol{Z}$, 总有

$$|N(\alpha)| = |(x^2 - Dy^2)/4| \geqslant |D|/4.$$

故若 $h = 1$, 素数 $p < |D|/4$, $\wp = \pi A$ 为 p 在 K 的素理想因子，则

$$p^f = N\wp = |N(\pi)| \geqslant |D|/4,$$

于是 $f = f(\wp|p) = 2$, 故 $(D/p) = -1$, $\pi = p$. 这一事实将多次使用.

现设 $h = 1$, $|D| > 9$, $|D|/4 > 2$. 于是由上述知 $(D/2) = -1$ 即 $D \equiv 5 (\mathrm{mod} 8)$. 特别这说明对 $11 < |D| \leqslant 19$ 类数不能是 1.

再设 $h = 1$, $|D| > 19$, $|D|/4 > 5$. 不必考虑 $|D| = 20$, 因为此时由 $C_K = (2/\pi)\sqrt{20} < 3$ 及 2 分歧可知 $h(-5) = 2$. 于是由上述知 $(D/2) = (D/3) = (D/5) = -1$, 即 $D \equiv 5 (\mathrm{mod} 8)$, $D \equiv -1 (\mathrm{mod} 3)$, $D \equiv 2$ 或 $3 (\mathrm{mod} 5)$. 故 $D \equiv -43$ 或 $-67 (\mathrm{mod} 120)$. 对 $|D| < 520$ 只可能有 $D = -43, -67, -163, -187, -283, -307, -403, -427$. 但 D 必须是素数，否则 D 含有素因子 $p < \sqrt{|D|} < |D|/4$, 从而由上述知 $(D/p) = -1$, 与 p 分歧矛盾. 因 $403 = (13)(31)$, $427 = (7)(61)$, $-187 \equiv 3^2 (\mathrm{mod} 7)$, $-283 \equiv 2^2 (\mathrm{mod} 7)$, $-307 \equiv 1^2 (\mathrm{mod} 7)$, 故只剩下 $D = -43, -67, -163$.

对于 $D = -163$, 有 $C_K < 9$, 而 $p = 2, 3, 5, 7$ 使 $(-163/p) = -1$, 故惯性，皆为主理想，在同一平凡类，故 $h(-163) = 1$. 对 $D = -43$ 和 -67 同样可证. □

注记 1 (1) 定理1最初是由 Gauss 猜想，Gauss 并算得这9个虚二次域的类数为1. 但其余虚二次域的类数均大于1这一事实，长期得不到解决，直到 1966 ~ 1967 年才由 Baker 和 Stark 独立证出，从而获得 Fieds 奖([St],[Ba]).

(2) Gauss 还猜想，具有任一给定类数 h 的虚二次域的个数 $G(h)$ 是有限数. 在 1971 年，Baker 和 Stark 又分别证明了 $G(2)=18$. 1983 年，Goldfeld - Gross - Zagier 得出惊人的结果：任给 $\epsilon>0$ 均存在一个可有效计算的常数 $c>0$ 使得

$$h(D)>c(\log|D|)^{1-\epsilon}.$$

这就彻底解决了 Gauss 虚二次域类数猜想(只差有限步计算，即算得右方 >1).

(3) 对于实二次域，Gauss 猜想：有无限多个 $d>0$ 使 $h(d)=1$. 这一猜想至今远未解决.

定理 2 对于判别式 $1<D<100$，除 4 个 D 值之外均有 $h(D)=1$. 四个例外是 $D=40, 60, 65, 85$，均有 $h(D)=2$.

证明 注意此时 $C_K=\frac{1}{2}\sqrt{|D|}<\frac{1}{2}\sqrt{100}=5$. 故每个理想类中必有整理想 J 使 $N(J)<5$，故 J 只能是 2 或 3 的素理想因子.

(i) 设 $D<16$，则 $C_K<2$，故必有 $h=1$.

(ii) 设 $16<D<36$，则 $C_K<3$，故只要考虑 2 的因子 $J=\wp$. 若 2 惯性，则 $N\wp=N(2)=4>C_K$，故必 $h=1$. 还剩下 $D=17, 24, 28, 33$. 对这些情况，$\wp=(\alpha)$ 均是主理想，因为 $N(\alpha)=N((x+y\sqrt{D})/2)=(x^2-y^2D)/4=\pm 2$ 分别有整

解(3, 1), (4, 1), (6, 1), (5, 1). 故均有 $h=1$.

(iii) 设 $36<D<100$. $C_K<\frac{1}{2}\sqrt{100}=5$. 同上知当 $(D/3)=-1$ 时必有 $h=1$.

对 $D=40$, $(2)=\wp_2^2$, $(3)=\wp_3\overline{\wp}_3$, 故非单位理想类由 $\wp_2$, $\wp_3$, 或 $\overline{\wp}_3$ 代表, 但 $x^2-10y^2=\pm 6$ 有整解, 故 $\wp_2\wp_3$ 和 $\overline{\wp_2\wp_3}=\wp_2\overline{\wp}_3$ 均为主理想. 以 $[\wp]$ 表示 $\wp$ 代表的理想类, 则 $[\wp_2][\wp_3]^{-1}=[\wp_2][\overline{\wp}_3]=[\wp_2\overline{\wp}_3]=1$, 故 $[\wp_2]=[\wp_3]$, 故 $[\overline{\wp}_3]=[\wp_3]^{-1}=[\wp_2]^{-1}=[\wp_2]=[\wp_3]$, 即知 $h(40)=2$.

对 $D=57$, $(x^2-57y^2)/4=\pm 2$ 有解 (7, 1), 故 2 的因子为主理想. 对方程 $(x^2-57y^2)/4=\pm 3$ 即 $x^2-57y^2=\pm 12$, 首先求 $0\leqslant s\leqslant 12/2$ 使 $s^2\equiv 57((\mathrm{mod}\ 12)$, 得 $s=3$, 故知 $(s^2-57)/12=-2^2$. 因 $x^2-57y^2=\pm 1$ 总有解, 故 $x^2-57y^2=\pm 2^2$ 总有解, 设为 (x_0, y_0). 于是, $(57y_0\pm sx_0)/4$, $(x_0\pm sy_0)/4)$ 为 $x^2-57y^2=\pm 12$ 的解. 这说明 3 的理想因子为主理想, 故 $h(57)=1$.

其余情形可类似得出, 读者可一试. □

关于实二次域 $\boldsymbol{Q}(\sqrt{d})$ 的类群 $H(d)$ 和类数 $h(d)$, 以及 Gauss 猜想等问题, 还远未解决. 但也已经有许多结果. 有许多关于类数 $h(d)=1$ 的判则, 例如[Zh2](及所引文献)中给出不少判则, 特别有: 若 $d=s^2+r$, $|r|=1$ 或 4, 则 $h(d)=1$ 当且仅当小于 $\sqrt{d-1}/2$ 的素数 p 在 K 均惯性. [Zh3~4]中给出许多系列(无限多个)实二次域 $\boldsymbol{Q}(\sqrt{d})$, 使其类群均含(任意) n 阶循环子群(特别 $n\,|\,h(d)$). 例如 $d=(z^n+t-1)^2+4t\quad(t\,|\,z^n-1$, z 奇), $d=(4z^n+t-1)^2/4+t\quad(t\,|\,4z^n-1,\ d\neq t)$. 特别这就用简单方法证明了: 对任意给定的 n, 类群含 n 阶循环子群的实二

次域有无限多个. 取 $t=1$ 则特别知对 $d=z^{2n}+4$ 和 $4z^{2n}+1$ 等，$H(d)$含 n 阶循环子群. [Lu]和[Zh5]给出了许多类数同余公式，例如，若 $\varepsilon=t+u\sqrt{d}$ 为 $\boldsymbol{Q}(\sqrt{d})$的基本单位，则当 $d\equiv 3 \pmod 8$时有 $2h(-m)\equiv 3tuh(m) \pmod 8$；当 $d\equiv 7 \pmod 8$ 时，$tuh(d)\equiv 0 \pmod 8$.

习　题

1. 证明 (1) 对于 $d=-15, -20, -24, -35, -40$ 有 $h(d)=2$.

(2) 对于 $d=-23, -31$ 有 $h(d)=3$.

(3) $h(-39)=4$.

7.3.1　二次域的单位和(严义)类数表

以下列出二次域 $K=\boldsymbol{Q}(\sqrt{d})$的类数和基本单位，其中 d 为无平方因子整数，$|d|<100$.

K 的两个理想 I, J 称为**严义等价**的，是指存在 $\alpha\in K$ 使 $I=\alpha J$ 且 $N(\alpha)>0$(其中 $N=N_{K/Q}$). K 的(分式)理想按严义等价分类，等价类集称为**严义(理想)类群**，记为 $H^+(K)$，$h^+=\# H^+$ 称为**严义(理想)类数**. 通常的类群和类数记为 H 和 h. 当 $d<0$ 时，任一 $\alpha\in K$ 满足 $N(\alpha)>0$，故 $H^+=H$. 当 $d>0$ 时，$N(\sqrt{d})=-d<0$，故 $H^+=H$ 当且仅当理想$(\sqrt{d})=(1)$，即存在单位 ε 使 $N(\varepsilon)=-1$. 当 K 的基本单位的范 $N(\varepsilon)=+1$ 时，$h^+=2h$，且有正合列：

$$1\to\{(1), (\sqrt{d})\}\to H^+\to H\to 1.$$

对于 $N(\varepsilon)=-1$ 情形，当且仅当 $d=a^2+b^2(a, b\in\mathbf{Z})$时 $H^+\neq H\times\mathbf{Z}/2\mathbf{Z}$(此时 h 总为偶数). 例如 $d=34$ 即如此(100 以内只有此例).

表 1　实二次域 $Q(\sqrt{d})(1<d<100)$

($h(h^+)$为(严义)类数，(m, n)指相应类群同构于 $\mathbf{Z}/m\mathbf{Z}\times\mathbf{Z}/n\mathbf{Z}$)

d	基本单位 ε	$N(\varepsilon)$	h	h^+
2	$1+\sqrt{2}$	-1	1	1
3	$2+\sqrt{3}$	$+1$	1	2
5	$(1+\sqrt{5})/2$	1	1	1
6	$5+\sqrt{6}$	$+1$	1	2
7	$8+3\sqrt{7}$	$+1$	1	2
10	$3+\sqrt{10}$	-1	2	2
11	$10+3\sqrt{11}$	$+1$	1	2
13	$(3+\sqrt{13})/2$	-1	1	1
14	$15+4\sqrt{14}$	$+1$	1	2
15	$4+\sqrt{15}$	$+1$	2	4(2, 2)
17	$4+\sqrt{17}$	-1	1	1
19	$170+39\sqrt{19}$	$+1$	1	2
21	$(5+\sqrt{21})/2$	$+1$	1	2
22	$197+42\sqrt{22}$	$+1$	1	2
23	$24+5\sqrt{23}$	$+1$	1	2
26	$5+\sqrt{26}$	-1	2	2

d	基本单位 ε	$N(\varepsilon)$	h	h^+
29	$(5+\sqrt{29})/2$	-1	1	1
30	$11+2\sqrt{30}$	$+1$	2	4(2, 2)
31	$11520+273\sqrt{31}$	$+1$	1	2
33	$23+4\sqrt{33}$	$+1$	1	2
34	$35+6\sqrt{34}$	$+1$	2	4(4)
35	$6+\sqrt{35}$	$+1$	2	4(2, 2)
37	$6+\sqrt{37}$	-1	1	1
38	$37+6\sqrt{38}$	$+1$	1	2
39	$25+4\sqrt{39}$	$+1$	2	4(2, 2)
41	$32+5\sqrt{41}$	-1	1	1
42	$13+2\sqrt{42}$	-1	2	4(2, 2)
43	$3482+531\sqrt{43}$	$+1$	1	2
46	$24335+3588\sqrt{46}$	$+1$	1	2
47	$48+7\sqrt{47}$	$+1$	1	2
51	$50+7\sqrt{51}$	$+1$	2	4(2, 2)
53	$(7+\sqrt{53})/2$	-1	1	1
55	$89+12\sqrt{55}$	$+1$	2	4(2, 2)
57	$151+20\sqrt{57}$	$+1$	1	2
58	$99+13\sqrt{58}$	-1	2	2

d	基本单位 ε	$N(\varepsilon)$	h	h^+
59	$530+69\sqrt{59}$	$+1$	1	2
61	$(39+5\sqrt{33})/2$	-1	1	1
62	$63+8\sqrt{62}$	$+1$	1	2
65	$8+\sqrt{65}$	-1	2	2
66	$65+8\sqrt{66}$	$+1$	2	4(2, 2)
67	$48842+5967\sqrt{67}$	$+1$	1	2
69	$(25+3\sqrt{69})/2$	$+1$	1	2
70	$251+30\sqrt{70}$	$+1$	2	4(2, 2)
71	$3480+413\sqrt{71}$	$+1$	1	2
73	$1068+125\sqrt{73}$	-1	1	1
74	$43+5\sqrt{74}$	-1	2	2
77	$(9+\sqrt{77})/2$	$+1$	1	2
78	$53+6\sqrt{78}$	$+1$	2	4(2, 2)
79	$80+9\sqrt{79}$	$+1$	3	6(2, 3)
82	$(9+\sqrt{82})/2$	-1	4(4)	4(4)
83	$82+9\sqrt{83}$	$+1$	1	2
85	$9+\sqrt{85}$	-1	2	2
86	$10405+1122\sqrt{86}$	$+1$	1	2
87	$28+3\sqrt{87}$	$+1$	2	4(2, 2)

d	基本单位 ε	$N(\varepsilon)$	h	h^+
89	$500+53\sqrt{89}$	-1	1	1
91	$1574+165\sqrt{91}$	$+1$	2	4(2, 2)
93	$(29+3\sqrt{93})/2$	$+1$	1	2
94	$2143295+221064\sqrt{94}$	$+1$	1	2
95	$39+4\sqrt{95}$	$+1$	2	4(2, 2)
97	$5604+569\sqrt{97}$	-1	1	1

表 2　虚二次域 $Q(\sqrt{d})$ 类数 h

（其中 $h=m\times n$ 或 m 是指类群 $H\cong \mathbf{Z}/m\times\mathbf{Z}/n$ 或 $\mathbf{Z}/m\mathbf{Z}$）

$-d$	1	2	3	5	6	7	10	11	13	14	15	17
h	1	1	1	2	2	1	2	1	2	4	2	4

19	21	22	23	26	29	30	31	33	34	35	37	38
1	2×2	2	3	6	6	2×2	3	2×2	4	2	2	6

39	41	42	43	46	47	51	53	55	57	58	59	61
4	8	2×2	1	4	5	2	6	4	2×2	2	3	3×2

62	65	66	67	69	70	71	73	74	77	78	79	82
8	4×2	4×2	1	4×2	2×2	7	4	5×2	4×2	2×2	5	4

83	85	86	87	89	91	93	94	95	97
3	2×2	10	6	12	2	2×2	8	8	4

§7.4 分圆域中的素分解及应用

设方程 $X^m-1=0$ $(m>2)$ 在复数域 $\boldsymbol{C}$ 中根为 $1, \zeta, \cdots, \zeta^{m-1}$，称为 m 次单位根(也记 $\zeta=\zeta_m$)，它们形成一个循环群 W，其生成元称为 m 次本原单位根. ζ^i 为本原单位根当且仅当 $(i, m)=1$. 域 $K=\boldsymbol{Q}(\zeta_m)$ 称为 m 级分圆域(m-th cyclotomic field).

引理 1 (1) $K=\boldsymbol{Q}(\zeta_m)$ 是 $\boldsymbol{Q}$ 的 $\varphi(m)$ 次 Abel 扩张.

(2) $\mathrm{Gal}(K/\boldsymbol{Q}) \cong (\mathbf{Z}/m\mathbf{Z})^*$.

(3) $\Phi_m(X)=\prod\limits_{\substack{(a,m)=1\\1\leqslant a<m}}(X-\zeta^a)$ 在 $\boldsymbol{Q}$ 上不可约.

(4) $(-1)^{(m-1)}m^m=\prod\limits_{j\neq i}(\zeta^i-\zeta^j)$.

证明 显然 K 是 X^m-1 的分裂域，故是 Galois 扩张. 设 $f(X)$ 是 ζ 在 $\boldsymbol{Q}$ 上的极小多项式，自然 $f(X)\mid X^m-1$. 因 $f(X)$ 的任一根生成 K，故必为 m 次本原单位根. 故对任一 $\sigma\in G=\mathrm{Gal}(K/\boldsymbol{Q})$，必有 $\sigma\zeta=\zeta^a$，其中 a 为正整数，$1\leqslant a<m$，$(a, m)=1$. 于是 $\sigma\longmapsto a$ 显然是 G 到 $(\mathbf{Z}/m\mathbf{Z})^*$ (即 $\mathbf{Z}/m\mathbf{Z}$)的单位群)中的单射.

现证明每个本原单位根 ζ^a 均是 $f(X)$ 的根. 为此只需证明：若 w 是 $f(X)$ 的根，则 w^p 也是 $f(X)$ 的根(素数 $p\nmid m$). 因 $f(X)\in\mathbf{Z}[X]$，故 $f(X^p)\equiv(f(X))^p \pmod p$，从而 $p\mid f(w^p)$，而由

$$X^m-1=\prod_{j=0}^{m-1}(X-\zeta^j)$$

知

$$\prod_{j=0}^{m-1}\zeta^j = (-1)^{m-1}.$$

由微商$(X^m-1)'=mX^{m-1}$，代入$X=\zeta^i$知

$$m\zeta^{i(m-1)} = \prod_{j(\neq i)}(\zeta^i - \zeta^j).$$

故

$$(-1)^{m-1}m^m = \prod_{j\neq i}(\zeta^i - \zeta^j).$$

因$w^p=\zeta^i$对某i成立，故$f(w^p)$是某些$\zeta^i-\zeta^j$的积，故知$f(w^p)\mid m^m$，与$p\nmid m$矛盾. □

引理1中的$\Phi_m(X)$称为分圆多项式，是$\mathbf{Z}$上$\varphi(m)$次不可约多项式，以所有m次本原单位根为根，故可得X^m-1的不可约分解：

$$X^m - 1 = \prod_{d\mid m}\Phi_d(X)$$

于是由Möbius反转公式可得

$$\Phi_m = \prod_{d\mid m}(X^{m/d} - 1)^{\mu(d)}$$

其中μ为Möbius函数(即当d含平方因子时$\mu(d)=0$，否则$\mu(d)=(-1)^r$，r为d的素因子个数，$\mu(1)=1$).

由引理1(2)可知，若$m=p^s$为奇素数之幂，则K为循环域. 若$m=2^s(s\geqslant 3)$，则$\mathrm{Gal}(K/\boldsymbol{Q})=\langle\tau\rangle\times\langle\sigma\rangle$，其中$\tau$为2阶元，$\tau(\zeta)=\zeta^{-1}$. σ为2^{s-2}阶，$\sigma\zeta=\zeta^5$.

引理2 (1) 分圆域K的判别式$D(K)$是m^m的因子.

(2) 设$p\nmid m$，σ_p是相应于p的K的Frobenius自同构，则$\sigma_p(\zeta)=\zeta^p$.

(3) 设$p\nmid m$，$\zeta^a\equiv\zeta^b(\mathrm{mod}\ pO_K)$，则$\zeta^a=\zeta^b$. $(a, b\in\mathbf{Z})$.

证 (1) $D(K)$ 整除 $\mathrm{Disc}(1,\zeta,\cdots,\zeta^{\varphi(m)-1})$，后者又整除 $\prod_{i\neq j}(\zeta^i-\zeta^j)=\pm m^m$.

(2) 按定义 $\sigma_p(\zeta)\equiv\zeta^p \pmod{pO_K}$，而 $\sigma_p(\zeta)$ 应当为某本原单位根 ζ^a，故 $\sigma_p(\zeta)=\zeta^a\equiv\zeta^p \pmod{pO_K}$. 再由(3)即得.

(3) 由 $\zeta^a\equiv\zeta^b$ 知 $\zeta^{a-b}\equiv 1 \pmod{pO_K}$，故 $p\mid(1-\zeta^{a-b})$. 而由 $(X^m-1)/(X-1)=\prod_{i=1}^{m-1}(X-\zeta^i)$，以 $X=1$ 代入知

$$m=\prod_{i=1}^{m-1}(1-\zeta^i).$$

因 $p\nmid m$，故若 $\zeta^a\neq\zeta^b$ 即 $1-\zeta^{a-b}\neq 0$ 则得出矛盾. □

定理 1 (1) 设素数 $p\nmid m$，则 p 在 $K=\boldsymbol{Q}(\zeta_m)$ 不分歧且分解为 $(p)=\wp_1\cdots\wp_g$，剩余类次数 $f=f(\wp_i|p)$ 是使 $p^f\equiv 1 \pmod m$ 最小正整数 $(1\leqslant i\leqslant g)$，$fg=\varphi(m)$. 特别，素数 p 在 $\boldsymbol{Q}(\zeta_m)$ 完全分裂当且仅当 $p\equiv 1 \pmod m$.

(2) 设 $m=p^s$ 为素数幂，则 p 在 K 完全分歧，$\wp=(1-\zeta)$ 为 p 的唯一素理想因子，即 $(p)=(1-\zeta)^{\varphi(p^s)}$.

(3) 若 $m=p^s m'$，$(m',p)=1$，$s\geqslant 1$. 则素数 p 在 K 分解为

$$(p)=(\wp_1\cdots\wp_g)^{\varphi(p^s)},$$

$f=f(\wp_i|p)$ 是使 $p^f\equiv 1 \pmod{m'}$ 成立的最小正整数，$fg=\varphi(m')$，$\wp_i$ 为 K 的互异素理想 $(1\leqslant i\leqslant g)$.

证 (1) 由引理 2 知 $p\nmid D(K)$，故 p 不分歧，f 是 Frobenius 自同构 σ_p 的阶. 而 $\sigma_p{}^f=1$ 相当于 $\sigma_p{}^f(\zeta)=\zeta$，即 $\zeta^{p^f}=\zeta$，即 $p^f\equiv 1(\mathrm{mod}\ m)$.

(2) $$\Phi_{p^s}(X)=\prod_{(i,p^s)=1}(X-\zeta^i)=\frac{X^{p^s}-1}{X^{p^{s-1}}-1}$$
$$=X^{p^{s-1}(p-1)}+\cdots+X^{p^{s-1}}+1 \qquad (*)$$

以 $X=1$ 代入知

$$p=\prod_{(i,p^s)=1}(1-\zeta^i)$$

每个 $1-\zeta^i$ 与 $1-\zeta$ 只差单位倍，这是因为 $(1-\zeta^i)/(1-\zeta)=\zeta^{i-1}+\cdots+\zeta+1\in O_K$，而 $(1-\zeta)/(1-\zeta^i)=(1-(\zeta^i)^j)/(1-\zeta^i)\in O_K$.

(3) 由 $\boldsymbol{Q}(\zeta_m)=\boldsymbol{Q}(\zeta_{m'})\boldsymbol{Q}(\zeta_{p^s})$即得.

Kronecker—Weber 定理断言：每个 Abel 数域 F 均含于某一分圆域之中. 这是类域论的一个直接推论，不过也可用初等方法证明(见[Ma]或[Zh6]). 但有趣的是，对于二次数域 F，我们可以立刻证明，并由此可直接得出二次互反律.

定理 2 (1) 设 $m=p$ 为奇素数，则 $K=\boldsymbol{Q}(\zeta_p)$含有唯一的二次域 F，即

$$F=\boldsymbol{Q}(\sqrt{(-1)^{(p-1)/2}p}).$$

(2) 每个二次域 $F=\boldsymbol{Q}(\sqrt{d})$均含于 $D=|\mathrm{Disc}(F)|$级分圆域 $\boldsymbol{Q}(\zeta_D)$中，且 D 是使 $F\subset\boldsymbol{Q}(\zeta_m)$的 m 的最小值(称为 F 的导子).

证 (1)$\boldsymbol{Q}(\zeta_p)$的 Galois 群是 $p-1$ 阶循环群，故有唯一的

指数为 2 的子群，故 $\boldsymbol{Q}(\zeta_p)$ 有唯一的二次子域. 设 $F=\boldsymbol{Q}(\sqrt{d})$，$d$ 为无平方因子整数. 其判别式 $D(F)$ 必为 $D(K)$ 的因子，从而为 p^p 的因子，故 $D(F)=\pm p=d$. 若 $p\equiv1((\bmod 4)$，则 $d=p$. 若 $p\equiv-1(\bmod 4)$，则 $d=-p$，故

$$d=(-1)^{(p-1)/2}p.$$

(2) 设 $d=\pm 2^t\prod_j(-1)^{(p_j-1)/2}p_j$，其中 $t=0$ 或 1，p_j 为奇素数. 记 $d'=\prod_j p_j$. 因 $\zeta_4=i=\sqrt{-1}$，$\zeta_8=(1+i)/\sqrt{2}$ (从而 $\sqrt{2}=\zeta_8+\zeta_8{}^{-1}$)，故总有

$$\boldsymbol{Q}(\sqrt{d})\subset\boldsymbol{Q}(\zeta_{8d'}).$$

使 $\boldsymbol{Q}(\sqrt{d})\subset\boldsymbol{Q}(\zeta_m)$ 的最小 m 值 m_o 分情形如下：

(1) 若 $d\equiv1(\bmod 4)$，则 $\pm2^t=1$，$m_o=d'=\pm d$，$D(F)=d$.

(2) 若 $d\equiv-1(\bmod 4)$，则 $\pm2^t=-1$，$m_o=4d'=\pm4d$，$D(F)=4d$.

(3) 若 $d\equiv2((\bmod 4)$，则 $\pm2^t=\pm2$，$m_o=8d'=\pm4d$，$D(F)=4d$. □

引理 3 记号如定理 2(1)，设素数 $q\neq p$，则

(1) q 在 F 分裂 $\Leftrightarrow q$ 在 $K=\boldsymbol{Q}(\zeta_p)$ 有偶数 g 个素理想因子.

(2) q 在 F 分裂 $\Leftrightarrow(q/p)=1$.

证 (1)$\Rightarrow$: $qO_F=\wp\overline{\wp}$，$\overline{\wp}$ 为 $\wp$ 的共轭，再在 K 中分解 $\wp$，$\overline{\wp}$ 即可.

$\Leftarrow$: K 为循环域，q 的分裂域 K^d 为偶数 g 次，故 $K^d\supset F$.

(2) q 分裂 $\Leftrightarrow g$ 为偶数 $(fg=p-1)\Leftrightarrow f\mid(p-1)/2\Leftrightarrow q^{(p-1)/2}$

$\equiv 1 \pmod p$（定理 1(1)）$\Leftrightarrow (q/p)\equiv 1 \pmod p \Leftrightarrow (q/p)=1$. 最后两步用到 Euler 公式：$(a/p)\equiv a^{(p-1)/2} \pmod p$. 这是由于，模 p 的二次剩余共 $(p-1)/2$ 个，故恰为满足 $a^{(p-1)/2}\equiv 1 \pmod p$ 的全部 a. 而由 $0\equiv a^{p-1}-1=(a^{(p-1)/2}-1)(a^{(p-1)/2}+1) \pmod p$ 知道，非二次剩余 a 恰为满足 $a^{(p-1)/2}\equiv -1 \pmod p$ 全体 a.

系 1（二次互反律） 设 p, q 为互异奇素数，则 Legendre 符号满足

(i) $(-1/p)=(-1)^{(p-1)/2}$;

(ii) $(2/p)=(-1)^{(p^2-1)/8}$;

(iii) $(q/p)(p/q)=(-1)^{(p-1)(q-1)/4}$.

证 (i)由 Euler 公式，$(-1/p)\equiv(-1)^{(p-1)/2} \pmod p$，即为(i).

(ii) $(2/p)=1$ 相当于 2 在 F 中分裂（见定理 2），即 $(-1)^{(p-1)/2}p\equiv 1 \pmod 8$，即 $p\equiv\pm 1 \pmod 8$，即 $p^2\equiv 1 \pmod{16}$，即 $(-1)^{(p^2-1)/8}=1$.

(iii) $(q/p)=1$ 相当于 q 在 F 中分裂（引理 3），即 $(d/q)=((-1)^{(p-1)/2}p/q)=1$. 即得.

习　题

1. 设 p 为奇素数，d 为 $p-1$ 的因子，F_d 是 $\boldsymbol{Q}(\zeta_p)$ 的 d 次子域. 证明素数 $q(\neq p)$ 是 d 次幂 $\pmod p$ 当且仅当 q 在 F_d 中分裂（提示：考虑 q 的分解，用 Frobenius).

§7.5　分圆域的整基与判别式

定理 1 设 $K=\boldsymbol{Q}(\zeta)$，$\zeta=\zeta_m$ 为 m 次本原单位根. 则

(1) $O_K=\mathbf{Z}[\zeta]$，即$\{1, \zeta, \cdots, \zeta^{\varphi(m)-1}\}$是 $K/\boldsymbol{Q}$ 的整基.

(2) K 的绝对判别式为

$$D(K) = (-1)^{\varphi(m)/2} m^{\varphi(m)} / \prod_{p|m} p^{\varphi(m)/(p-1)}$$

特别当 $m=p^s$ 时，

$$D(K)=\pm p^a, \qquad a=p^{s-1}(ps-s-1);$$

当 $p^s=4$ 或 $p\equiv 3 \pmod 4$时，$\pm$取负号，否则为正号.

证 设 p 为素数，$\wp$ 为其在 K 的任一素理想因子，$K_\wp$ 为局部域，$O_\wp$ 为其整数环. 若 $O_\wp=\mathbf{Z}_p[\zeta]$且 $D_\wp=\mathrm{Disc}(K_\wp/\boldsymbol{Q}_p)$ 为定理中 $D(K)$的$\wp$一分量，则称定理在$\wp$成立. 若在所有$\wp\mid p$ 成立则也称在 p 成立. 只需证明定理在所有 p 成立.

(1)先设 $p\nmid m$，ζ 的极小多项式 $f(X)=\Phi_m(X)$. 设 $X^m-1=f(X)g(X)$，微商并以 $X=\zeta$ 代入得

$$m\zeta^{m-1}=f'(\zeta)g(\zeta),$$

故 $f'(\zeta)$在 p 为单位，由局部域中差分 §5. 6 命题 2(2)知

$$\mathbf{Z}_p[\zeta]\subset O_\wp\subset O_\wp^*\subset \mathbf{Z}_p[\zeta]^*=\mathbf{Z}_p[\zeta]/f'(\zeta)=\mathbf{Z}_p[\zeta],$$

即知在 p 成立.

以上推理和结论显然也适用于相对分圆扩张 $K=F[\zeta_m]$.

再设 $m=p^s$ 为素数幂. 于是局部扩张 $K_\wp/\boldsymbol{Q}_p$ 完全分歧，$\wp=(1-\zeta)$. 由局部域的完全分歧扩张理论知$\{1, 1-\zeta, \cdots, (1-\zeta)^{\varphi(m)-1}\}$是 $K_\wp/\boldsymbol{Q}_p$ 的整基，再由 $\mathbf{Z}_p[1-\zeta]=\mathbf{Z}_p[\zeta]$即知(1)在 p 正确，对 $m=p^s$ 正确.

对一般情形，设 $m=m'p^s$，$(m', p)=1$，设$\wp'$为 p 在 $K'=\boldsymbol{Q}(\zeta_{p^s})$的唯一素因子，则 $O_{\wp'}=\mathbf{Z}_p[\zeta_{p^s}]$，$O_\wp=O_{\wp'}[\zeta_{m'}]=\mathbf{Z}_p[\zeta_{p^s}, \zeta_{m'}]=\mathbf{Z}_p[\zeta_m]$.

(2)先设 $m=p^s$，记 $n=\varphi(p^s)$. 由§7.4定理1(2)的证明中(*)式知

$$(\zeta^{p^{s-1}}-1)f'(\zeta)=p^s\zeta^{p^s-1},$$

即得 $f'(\zeta)$，注意 $D(K)=(-1)^{n(n-1)/2}N_{K/Q}(f'(\zeta))$.

$N(\zeta)=\prod\limits_{(i,p)=1}\zeta^i=(-1)^n$. 又 $w=\zeta^{p^{s-1}}$ 是 p 次本原单位根. 故

$$N(1-w)=N_{Q(w)/Q}(1-w)^{[K:Q(w)]}$$
$$=\prod_{i=1}^{p-1}(1-w^i)^{n/(p-1)}=p^{n/(p-1)}.$$

即得定理.

再看一般情形，对 m 进行归纳. 设 $m=m'q^t$，q 为奇素数，$(q,m')=1$，$m'>2$. 设 $K'=Q(\zeta_{m'})$，$K^q=Q(\zeta_{q^t})$，于是由下式即得定理：

$$|D(K)|=|D(K')|^{\varphi(q^t)}|D(K^q)|^{\varphi(m')}.$$ □

习　题

1. 若 $(m,n)=1$，则 $Q(\zeta_m)\cap Q(\zeta_n)=Q$.

§7.6　分圆域的单位与类数

设分圆域 $K=Q(\zeta_m)$，$\zeta=\zeta_m$. 显然 K 到 C 的每个嵌入均为复嵌入(因为实单位仅有±1). 故 K 的独立自由单位个数为 $\varphi(m)/2-1$. 当 m 为奇数时，$-\zeta_m$ 为 $2m$ 次本原单位根，故 K 中单位根群为 $W=\langle-\zeta_m\rangle$，$2m$ 阶. 当 m 为偶数时，$W=\langle\zeta_m\rangle$ 为 m 阶群.

定理 1 (1)若 $m=p^s$ 为素数幂，则 $(1-\zeta^a)/(1-\zeta)$ 为单位(对任意与 m 互素的正整数 a).

(2)若 m 有两个以上不同素因子，则 $1-\zeta^a$ 是单位(对任意与 m 互素的正整数 a).

证 (1)见§7.4定理1(2)的证明.

(2)ζ^a 是本原单位根，故只需证 $1-\zeta$ 是单位. 记 $m=p^s m'$，$(m',p)=1$，$p^s>2$，$\zeta=\zeta_{p^s}\cdot\zeta_{m'}$. 则

$$X^{p^s}-1=\prod_{i=0}^{p^s-1}(X-\zeta_{p^s}^i),$$

$$X^{p^s}-\zeta_{m'}^{p^s}=\prod_{i=0}^{p^s-1}(X-\zeta_{p^s}^i\zeta_{m'}),$$

$$(1-\zeta_{m'}^{p^s})/(1-\zeta_{m'})=\prod_{i=1}^{p^s-1}(1-\zeta_{p^s}^i\zeta_{m'}).$$

若 $m'>2$ 是素数幂，则左边为单位，故右边也是单位，特别 $1-\zeta=1-\zeta_{p^s}\zeta_{m'}$ 为单位. 再对 m 的素因子个数归纳即得定理. □

复共轭映射 σ 是 K 的自同构，因 σ 是2阶元，故其固定子域是 $\varphi(m)/2$ 次域，记为 K^+，这是 K 的最大实子域. 因 $\boldsymbol{Q}(\zeta+\zeta^{-1})$ 是实域，而 $\zeta^2-(\zeta+\zeta^{-1})\zeta+1=0$，故

$$K^+=\boldsymbol{Q}(\zeta+\zeta^{-1}).$$

K^+ 的单位群 $U^+=\langle\pm1\rangle\times\boldsymbol{Z}^s$，它的自由秩 $s=\varphi(m)/2-1$，与 K 的单位群 U 的秩是一样的. 它们的基本单位系是否一样呢？有如下定理.

定理 2 设 $m=p^s$ 为奇素数 p 之幂，则 K^+ 的基本单位系也是 K 的基本单位系.

证 设 u 是 K 的单位，$\bar{u}$ 为其复共轭，则 $\bar{u}/u$ 是单位根（因其任意赋值均为 1）．记 $\zeta=\zeta_m$，则 ζ^2 也是 p^s 次本原单位根，K 的单位根群 $W=\langle -\zeta^2\rangle$，故存在整数 a 使 $\bar{u}/u=(-\zeta^2)^a=\pm\zeta^{2a}$，即 $\bar{u}\bar{\zeta}^a=\pm u\zeta^a$．若此式中负号成立，则 $u\zeta^a$ 在 K^+ 上的极小多项式为 $f(X)=X^2-u^2\zeta^{2a}$，差分 $f'(u\zeta^a)=2u\zeta^a$ 为 $\wp$－adic 单位（$\wp$ 为 p 在 K 中素因子），故 $\wp$ 在 K/K^+ 不分歧，这与 $\wp$ 在 $K/\boldsymbol{Q}$ 完全分歧矛盾．故知 $u^+=u\zeta^a$ 为实单位，$u=\zeta^{-a}u^+$． □

关于 $K=\boldsymbol{Q}(\zeta_m)$ 的类数 h_m，利用 Minkowski 常数易算得：当 $3\leqslant m\leqslant 10$ 时，$h_m=1$．可以证明当 $m\leqslant 19$ 时均有 $h_m=1$，且不再有其它的素数 $m=p$ 使 $h_p=1$．例如 $h_{23}=3$．

历史上，分圆域的类数与 Fermat 大定理关系密切．

定理 3 若奇素数 $p\nmid h_p$ （h_p 是 $\boldsymbol{Q}(\zeta_p)$ 的类数），则 Fermat 方程 $x^p+y^p=z^p$，$(xyz,\ p)=1$，无有理整数解．

证 先看 $p=3$．若 $3\nmid x$ 则 $x^3\equiv\pm 1 \pmod 9$．对 y,z 同样．故 $x^3+y^3\equiv -2,\ 0$，或 $2 \pmod 9$，故 Fermat 方程无解．对 $p=5$，考虑模 25 同样可证．当 $p\geqslant 5$ 时，若 $x\equiv y\equiv -z \pmod p$，则 $-2z^p\equiv z^p$，$3z^p\equiv 0 \pmod p$，与 $p\nmid 3z$ 矛盾．故我们总可设 $x\not\equiv y \pmod p$（否则重写为 $x^p+(-z)^p=(-y)^p$）．又显然可设 x,y,z 两两互素．我们需以下引理，记号如定理 3：

引理 1 (1) 理想 $(x+\zeta^i y)$，$i=0,\ 1,\ \cdots,\ p-1$，两两互素（其中 $x,\ y,\ z\in\boldsymbol{Z}$ 满足 $x^p+y^p=z^p$，$p\nmid xyz$）．

(2) 若 $\alpha\in\boldsymbol{Z}[\zeta]$，则 $\alpha^p\equiv a \pmod p$，$a\in\boldsymbol{Z}$．

(3) 设 $\alpha=a_0+a_1\zeta+\cdots+a_{p-1}\zeta^{p-1}$，$a_i\in\boldsymbol{Z}$ 且至少有一个为

0，若有理整数 $n|\alpha$，则 $n|a_j(0\leqslant j\leqslant p-1)$. 类似地，设所有的 $a_i\in\mathbf{Z}_p$ 且至少一个为 0，若 $p|\alpha$ 则 $p|a_j(0\leqslant j\leqslant p-1)$.

证 (1)设 $(x+\zeta^i y)$ 与 $(x+\zeta^j y)$ 有公共理想素因子 $\wp$，则 $\wp\,|(\zeta^i y-\zeta^j y)=w(1-\zeta)y$，其中 w 为单位，故 $\wp=(1-\zeta)$ 或 $\wp\,|y$；类似可知 $\wp\,|(\zeta^j(x+\zeta^i y)-\zeta^i(x+\zeta^j y))=w(1-\zeta)x$，故 $\wp=(1-\zeta)$ 或 $\wp\,|x$. 因 x，y 互素，故 $\wp=(1-\zeta)$. 于是 $x+y\equiv x+\zeta^i y\equiv 0(\bmod\ \wp)$，即 $x+y\equiv 0(\bmod\ p)$，故 $z^p=x^p+y^p\equiv x+y\equiv 0(\bmod\ p)$，故 $p|z$，矛盾！

(2) 设 $\alpha=b_0+b_1\zeta+\cdots+b_{p-2}\zeta^{p-2}$，则 $\alpha^p\equiv b_0{}^p+\cdots+(b_{p-2}\zeta^{p-2})^p=b_0{}^p+\cdots+b_{p-2}{}^p(\bmod\ p)$.

(3) $\{1,\zeta,\cdots,\zeta^{p-1}\}$ 中的任 $p-1$ 个元素是 $\mathbf{Z}[\zeta]$ 的 $\mathbf{Z}$-基，因有一个 $a_i=0$，故其余 a_j 是一个基中各元素的系数，故得第一个结论. 第二个结论类似可得.

继续定理 3 的证明. 设 Fermat 方程有解 x，y，z，将左边分解，考虑理想方程：

$$\prod_{i=0}^{p-1}(x+\zeta^i y)=(z)^p.$$

因左侧的理想两两互素，故每一个均为某理想 A_i 的 p 次幂：$(x+\zeta^i y)=A_i{}^p$ 因 $A_i{}^p$ 为主理想而 $p\nmid h_p$，故 A_i 必定为主理想. 设 $A_i=(\alpha_i)$，则 $(x+\zeta^i y)=(\alpha_i{}^p)$，$x+\zeta^i y=u\alpha_i{}^p$（$u$ 为单位）.（注意，此结果正是历史上以为 $\mathbf{Z}[\zeta]$ 是唯一析因环所想得到的）. 设 $i=1$ 而省去足标，则得 $x+\zeta y=u\alpha^p$. 定理 2 说明 $u=\zeta^r u_1$，其中 u_1 为实单位. 引理 1(2)说明 $\alpha^p\equiv a(\bmod\ p)$，故 $x+\zeta y=\zeta^r u_1\alpha^p\equiv\zeta^r u_1 a(\bmod\ p)$. 同时 $x+\bar\zeta y=\zeta^{-r}u_1\bar\alpha^p\equiv\zeta^{-r}u_1 a(\bmod\ p)$，故

$$\zeta^{-r}(x+\zeta y)\equiv\zeta^r(x+\bar\zeta y)\quad(\bmod\ p),$$

即

$$x+\zeta y-\zeta^{2r}x-\zeta^{2r-1}y\equiv 0 \pmod p. \qquad (*)$$

若 $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$互异，则引理 1(3)说明 $p\mid(x, y)$，不可能. 故它们并非互异. 因显然 $1\neq\zeta, \zeta^{2r}\neq\zeta^{2r-1}$，故有以下三种情形：

(1) $1=\zeta^{2r}$，$(*)$式化为 $\zeta y-\zeta^{p-1}y\equiv 0 \pmod p$. 由引理 1 知 $p\mid y$，与原设矛盾.

(2) $1=\zeta^{2r-1}$，$(*)$式化为 $(x-y)-(x-y)\zeta\equiv 0 \pmod p$，引理 1 说明 $p\mid(x-y)$，也与证明开始所说矛盾.

(3) $\zeta=\zeta^{2r-1}$，$(*)$式化为 $x-\zeta^2x\equiv 0 \pmod p$，故 $p\mid x$，矛盾. □

注记 对于 $p\mid xyz$ 的情形，定理 3 也可证明是成立的. 但是如何判断 $p\nmid h_p$ 呢？设 Bernoulli 数 B_n 由下式定义：

$$t/(e^t-1)=\sum_{n=0}^{\infty} B_n t^n/n!.$$

例如 $B_0=1$，$B_1=-\frac{1}{2}$，$B_2=\frac{1}{6}$，$B_3=0$，$B_{2k+1}=0$，$B_4=-\frac{1}{30}$，$B_6=\frac{1}{42}$. Kummer 证明了：

$$p\mid h_p \Leftrightarrow p\mid B_k \qquad (k=2, 4, 6, \cdots, p-3).$$

习　题

1. $\boldsymbol{Q}(\zeta_m+\zeta_m^{-1})$的整数环为 $\boldsymbol{Q}[\zeta_m+\zeta_m^{-1}]$.

2. 具体求出 $\boldsymbol{Q}(\zeta_8)$所含的 3 个二次子域.

3. 设 p 为奇素数，证明 $\boldsymbol{Q}(\zeta_{p^2})$有唯一的 p 次子域 K. 证明 $2^{p-1}\equiv 1 \pmod{p^2}$当且仅当 2 在 K 完全分裂.

第八章　特征与解析理论

§8.1　Dirichlet 特征

设 m 为正整数．群同态映射

$$\chi:\quad (\mathbf{Z}/m\mathbf{Z})^{*}\to C^{*}$$

称为一个模 m 的 Dirichlet **特征**(character)，简称 D-特征，或特征．这里 $G_m=(\mathbf{Z}/m\mathbf{Z})^{*}$ 为 $\mathbf{Z}/m\mathbf{Z}$ 中的单位乘法群．模 m 的 D—特征全体是一个乘法群，记为 $\hat{G}_m$．例如 $G_4=\{1,\ -1\}$，故 $\hat{G}_4=\{\chi_0,\chi_1\}$，其中 $\chi_0(-1)=1$，$\chi_1(-1)=-1$．若令 $\chi_0(a)=1(\forall\ a\in G_m)$，则 χ_0 是特征，称为主特征，常记为 $\chi_0=1$．此外，依 $\chi(-1)=+1$ 或-1，分别称 χ 为**偶特征**或**奇特征**．偶特征全体$(\hat{G}_m)^{+}$是 $\hat{G}_m$ 的子群，指数为 2.

若 $a\in\mathbf{Z}$ 与 m 互素，$\bar{a}\in\mathbf{Z}/m\mathbf{Z}$，也常记 $\chi(a)=\chi(\bar{a})$．当 $a\in\mathbf{Z}$ 与 m 不互素时，常记 $\chi(a)=0$.

设 $m=p^{s}$ 为奇素数 p 之幂，则 $G_m=\langle\bar{g}\rangle$是由原根 g 生成的 $\varphi(m)=(p-1)p^{s-1}$阶循环群．由于 $\bar{g}^{\varphi(m)}=1$ 故对任一 $\chi\in\hat{G}_m$ 均有

$$\chi(\bar{g})^{\varphi(m)}=\chi(\bar{g}^{\varphi(m)})=\chi(1)=1,$$

即 $\chi(\bar{g})$是 $\varphi(m)$次复单位根. 另一方面，令

$$\chi_j(\bar{g})=\zeta^j \qquad (j=0, 1, \cdots, \varphi(m)-1),$$

及 $\chi_j(\bar{g}^i)=\chi_j(\bar{g})^i=\zeta^{ij}$(其中 $\zeta=\zeta_{\varphi(m)}$)，则得到 $\varphi(m)$个模 m 特征 $\chi_0, \cdots, \chi_{\varphi(m)-1}$，它们恰为模 m 的全部特征(因为 $\chi(\bar{g})$只有这几种可能取值). 记 $\chi_1=\rho_{p^s}$，则 $\chi_j=\rho_{p^s}{}^j$，$\hat{G}_m=\langle\chi_1\rangle$.

再设 $m=2^s$. 当 $s=1$ 时显然只有主特征. 当 $s=2$ 时已知有 $\hat{G}_4=\{\chi_0, \chi_1\}$. 当 $s\geqslant 3$ 时，

$$G_{2^s}=\langle-\bar{1}\rangle\times\langle\bar{5}\rangle,$$

其中$\langle-\bar{1}\rangle$是 2 阶群，$\langle\bar{5}\rangle$是 $t=2^{s-2}$阶群，若

$$\bar{a}=(-\bar{1})^\delta(\bar{5})^i, \qquad (\delta=0, 1; i=0, \cdots, t-1),$$

则 $\chi(\bar{a})=\chi(-1)^\delta\chi(5)^i$，$\chi(-1)^2=1$，$\chi(5)^t=1$，故 $\chi(-1)=\pm 1$，$\chi(5)$是 t 次单位根，令

$$\chi_{ej}(\bar{a})=(-1)^{\delta e}\zeta_t^{ij} \qquad (e=0, 1; \qquad j=0, \cdots, t-1),$$

则得到 $\varphi(m)$个模 m 特征 χ_{ej}. 记 $\chi_{10}=\psi$，$\chi_{01}=\rho_{2^s}=\rho$，即 $\psi(-1)=-1$，$\rho(5)=\zeta_t$，$\chi_{ej}=\psi^e\rho^j$，则

$$\hat{G}_{2^s}=\langle\psi, \rho\rangle=\{1, \rho, \cdots, \rho^{t-1}, \psi, \psi\rho, \cdots, \psi\rho^{t-1}\}.$$

一般地，设

$$m=p_1^{s_1}p_2^{s_2}\cdots p_w^{s_w}=m_1\cdots m_w,$$

其中 p_i 为不同素数. 设 χ_{p_i}为模 m_i 的特征，则

$$\chi=\chi_{p_1}\chi_{p_2}\cdots\chi_{p_w}$$

为模 m 特征. 由此即得到 $\varphi(m)$个模 m 特征. 若 $p_1=2$，$s_1\geqslant 3$，则显然

$$\chi=\psi^e\rho_1^{j_1}\rho_2^{j_2}\cdots\rho_w^{j_w},$$

其中 $\rho_j=\rho_{m_j}$($0\leqslant j_1<2^{s_1-2}$，$0\leqslant j_i<\varphi(m_i)$ (当 $i\geqslant 2$)，$e=0, 1$)即

为模 m 的全部特征，亦即

$$\hat{G}_m = \hat{G}_{m_1} \times \cdots \times \hat{G}_{m_w}.$$

我们可对更一般的情形讨论如下.

对任一有限 Abel 群 G，定义 G 的特征为群同态映射 $\chi: G \to \mathbf{C}^*$. G 的特征全体记为 $\hat{G}$，是一个 Abel 群. G 可分解为循环群的直积

$$G = \langle g_1 \rangle \times \cdots \times \langle g_w \rangle,$$

于是

$$\hat{G} = \widehat{\langle g_1 \rangle} \times \cdots \times \widehat{\langle g_w \rangle},$$

而 φ 阶循环群 $\langle g \rangle$ 的特征群为 $\langle \rho \rangle$，也是 φ 阶循环群，因此我们得到群同构：

$$G \cong \hat{G}.$$

另一方面，G 也可看作是 $\hat{G}$ 的特征群，即对 $g \in G$ 和 $\chi \in \hat{G}$，定义 $g(\chi) = \chi(g)$. 因此有等同(或称为自然同构)：

$$\hat{\hat{G}} = G.$$

为了更好地表现 G 与 $\hat{G}$ 的这种相互对等的地位，宜记

$$(g, \chi) = g(\chi) = \chi(g).$$

因而我们自然就有了一个非退化配对

$$G \times \hat{G} \longrightarrow \mathbf{C}^*. \qquad (*)$$

G 和 $\hat{G}$ 的子群间有很好的对偶关系. 设 H 为 G 的子群，记

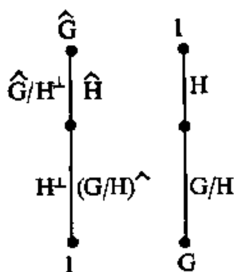
$$H^{\perp} = \{\chi \in \hat{G} \mid (h, \chi) = 1, \ \forall\ h \in H\},$$

称为 H 的正交补.

引理 1 (1) $H^{\perp} = (G/H)^{\wedge}$，

(2) $\hat{H}=\hat{G}/H^{\perp}$,

(3) $(H^{\perp})^{\perp}=H$.



证 (1) $\chi\in H^{\perp}\Leftrightarrow\chi(H)=1$

$\Leftrightarrow\chi\in(G/H)^{\wedge}$.

(2)限制映射 $\hat{G}\longrightarrow\hat{H}$ 的核为 $H^{\perp}$，只需再证它是满射. 由 $\# H^{\perp}=\#(G/H)^{\wedge}=\#(G/H)$，即知 $\#\hat{H}=\# H=\#(\hat{G}/H^{\perp})$.

(3)显然 $H\subset(H^{\perp})^{\perp}$，再因二者元素个数相同，即得所欲证. □

由于 G 与 $\hat{G}$ 的对偶性，引理 1 也有其对偶性的结果：对于 $\hat{G}$ 的子群 X，可同样定义 $X^{\perp}\subset G$，则 $X^{\perp}=(\hat{G}/X)^{\wedge}$，$\hat{X}=G/X^{\perp}$，$(X^{\perp})^{\perp}=X$. 引理 1 对局部紧 Abel 群也成立.

例 1 $G_6=(\mathbf{Z}/6\mathbf{Z})^*=\{\bar{1},-\bar{1}\}$，故 $\hat{G}_6=\{1,\chi\}$，$\chi(-1)=-1$.

例 2 $G_8=(\mathbf{Z}/8\mathbf{Z})^*=\{\bar{1},\bar{3},\bar{5},\bar{7}\}=\langle-\bar{1}\rangle\times\langle\bar{5}\rangle$. 故 $\hat{G}_8=\langle\psi,\rho\rangle=\{1,\rho,\psi,\psi\rho\}$. 由于 $\zeta_4=-1$，而 $\{\pm1;\pm5\}\equiv\{1,7;5,3\}(\text{mod}8)$，故有下表

	1	3	5	7
1	1	1	1	1
ρ	1	-1	-1	1
ψ	1	-1	1	-1
$\psi\rho$	1	1	-1	-1

例 3　$G_{16}=(\mathbf{Z}/16\mathbf{Z})^*=\langle -\bar{1}\rangle\times\langle\bar{5}\rangle$，$\hat{G}_{16}=\langle\psi,\rho\rangle$，$\zeta_t=\zeta_4=i$，$\rho(5)=i$，由于$\pm 1$，$\pm 5$，$\pm 5^2$，$\pm 5^3$ 模 16 分别同余于 1，15；5，11；9，7；13，3．故知

$\rho(1,3,5,7,9,11,13,15)=(1,-i,i,-1,-1,i,-i,1)$，

$\psi(1,3,5,7,9,11,13,15)=(1,-1,1,-1,1,-1,1,-1)$．□

若 m 是 n 的倍数，则模 n 特征 χ 诱导出模 m 特征：

$$(\mathbf{Z}/m\mathbf{Z})^*\longrightarrow(\mathbf{Z}/n\mathbf{Z})^*\xrightarrow{\chi}\boldsymbol{C}^*.$$

故 χ 也可看作模 m 特征．故 χ 的（定义）模不是一定的．χ 的最小模称为其**导子**(Conductor)，记为 f_χ 或 $\mathrm{con}(\chi)$．而 χ 称为模 f_χ 的**本原特征**(primitive character)，此时 χ 在 $\mathbf{Z}$ 上的取值以 f_χ 为周期．今后，均认为特征 χ 是以其导子 f_χ 为模的（除非特别说明），即均视为本原特征．

例 1 中的模 6 特征 χ 不是本原的，可由模 3 本原特征 χ_3 诱导得到，这里 $\chi_3(-1)=-1$．注意当考虑在 $\mathbf{Z}$ 上取值时，χ 与 χ_3 是有区别的，例如 $\chi_3(4)=\chi_3(1)=1$，而 $\chi(4)=1$（因为 4 与 6 不互素，而与 3 互素）．所以在 $\mathbf{Z}$ 上，本原特征取值为 0 的情况最少．例 2 中，ψ 对模 8 不是本原的，是模 4 本原特征，取值以 4 为周期．ρ 和 $\psi\rho$ 是模 8 本原特征．

设 χ_1 和 χ_2 的导子分别为 f_1，f_2．令模 $m=\mathrm{Lcm}\{f_1,f_2\}$的特征 χ 为：

$$\chi(a)=\chi_1(a)\chi_2(a),$$

χ 所决定的本原特征 χ^* 定义为 $\chi_1\chi_2$．注意积 $\chi_1\chi_2$ 与 χ 的导子相同，但可能不是 m．不过当 f_1 与 f_2 互素时，易知确有 $f_{\chi_1\chi_2}=f_1f_2$．

§8.2 域的特征群与素分解

设 $L=L_m=\boldsymbol{Q}(\zeta_m)$为分圆域，其 Galois 群可以等同于 $G=G_m=(\boldsymbol{Z}/m\boldsymbol{Z})^*$，即将 σ_i 等同于 i，其中 $\sigma_i(\zeta_m)=\zeta_m^i$. 所以模 m 的 Dirichlet 特征也就是域 L_m 的 Galois(群的)特征.

L 的子域全体$\{K\}$是一个格，它与 G 的子群格$\{H\}$之间反序 1∶1 对应(Galois 理论). 而 $\hat{G}$与 G 的子群格之间也是反序 1∶1 对应:$X\longmapsto H=X^{\perp}$(§1 引理 1). 所以 L 的子域格$\{K\}$与 $\hat{G}$的子群格$\{X\}$之间保序 1∶1 对应：

$$K\longleftrightarrow H\longleftrightarrow X,$$

即 K 对应于(对于上节配对(*))特征子群

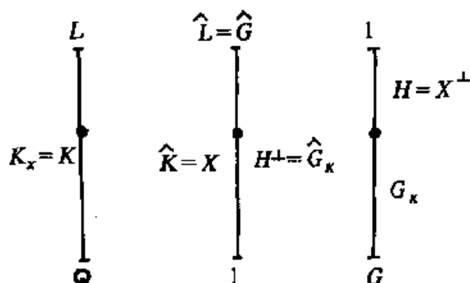
$$X=H^{\perp}=\{\chi\in\hat{G}\mid\chi(h)=1,\ 对\ h\in H=G(L/K)\},$$

记 $X=\hat{K}$，称为 K 的特征群，而任一特征子群 X 对应于一个子域

$$K=K_X=\{\alpha\in L\mid g(\alpha)=\alpha,\ 对\ g\in X^{\perp}\}.$$

自然有 $K_1\subset K_2\Leftrightarrow\hat{K}_1\subset\hat{K}_2$，$(K_1K_2)\hat{}=\hat{K}_1\hat{K}_2$.

若 $X=\langle\chi\rangle$是 χ 生成的循环群，χ 的导子为 $f=f_\chi$，则 $X\subset$



$\hat{G}_f=\widehat{(\mathbf{Z}/f\mathbf{Z})^*}$，$K_\chi\subset L=L_f$.

设 X 是一些 D—特征构成的任一群，令

$$m=\underset{\chi\in X}{\text{l.c.m}}\{f_\chi\},$$

则 $X\subset\hat{G}_m$，$K_X\subset L_m=\boldsymbol{Q}(\zeta_m)$，$m$ 称为 X 和 K_X 的**导子**. 显然 K_X 是 $H=\bigcap\limits_{\chi}\operatorname{Ker}\chi$ 的固定子域，由引理 1 及 $G_K=\operatorname{Gal}(K/\boldsymbol{Q})=G/H$，知 $\hat{G}_K=H^\perp=X$.

更进一步，设 $X=\hat{K}$，即 K 是特征群 X 对应的 Abel 域，则与上述同样易知，K 的子域格 $\{F\}$ 与 X 的子群格 $\{Y\}$ 之间是保序 1∶1 对应的，因为二者均与 $G_K=\operatorname{Gal}(K)$ 的子群格 $\{J\}$ 反序 1∶1 对应：

$$F\longleftrightarrow J\longleftrightarrow Y.$$

事实上，由于 $\hat{G}_K=X$，故有配对映射

$$G_K\times X\longrightarrow\boldsymbol{C}^*,\ (g,\chi)=\chi(g).\qquad(**)$$

对给定的 F，令

$$Y=\{\chi\in X\mid\chi(j)=1,\ \text{对 } j\in J=G(K/F)\},$$

则由引理 1 有（对配对(**)）：

$$Y=J^\perp=(G_K/J)\hat{}\ =\hat{G}_F$$

L　　$\hat{K}=\hat{X}$　　1

F　　Y　$\hat{G}_F$　　J

　　　　　　　　G_F

$\boldsymbol{Q}$　　1　　G_K

反之，对给定的Y，令

$$F=(Y^{\perp}\text{的固定子域}),$$

则$Y^{\perp}=G(K/F)=J$(Galois 理论)，故$Y=(Y^{\perp})^{\perp}=J^{\perp}=\hat{G}_F$.

例 1 $L_m=\boldsymbol{Q}(\zeta_m)$中的复共轭即为自同构$\sigma_{-1}:\zeta_m\longmapsto\zeta_m^{-1}$，在$G_m=(\mathbf{Z}/m\mathbf{Z})^*$中表示为$-1$. 子群$H=\langle -1\rangle\subset G_m$的固定子域为$L_m^+=\boldsymbol{Q}(\zeta_m+\zeta_m^{-1})$，$H$在$\hat{G}_m$中的正交补为

$$H^{\perp}=\{\chi\mid\chi(-1)=1\}=\hat{G}_m^+,$$

恰为偶特征全体. 故知$(L_m^+)^{\wedge}=(\hat{G}_m)^+$. 而$\chi\in G_m$对应的子域为实域$\Leftrightarrow\chi\in(-1)^{\perp}\Leftrightarrow\chi(-1)=1$，即$\chi$为偶特征. 所以偶特征也称为**实特征**. 例如在$\hat{G}_{16}$中(上节例 3)，ρ是偶特征，ψ是奇特征，故

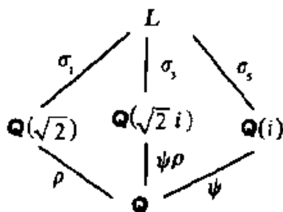
$$\hat{G}_{16}=\langle\rho\rangle\cup\psi\langle\rho\rangle,$$

$\langle\rho\rangle$对应L_{16}的 4 次实子域L_{16}^+，$L_{16}=L_{16}^+(\sqrt{-1})$.

例 2 $\hat{G}_8=\{1,\rho,\psi,\psi\rho\}$，其中$\rho(5)=-1$，$\rho(-1)=1$，$\rho(3)=-1$，$\rho(5)=1$，$\psi(-1)=-1$，$\psi(3)=-1$. 故$\langle\rho\rangle^{\perp}=\langle -1\rangle$，$\langle\psi\rangle^{\perp}=\langle 5\rangle$，$\langle\psi\rho\rangle^{\perp}=\langle 3\rangle$. 考虑

$$L_8=\boldsymbol{Q}((\sqrt{2}+\sqrt{2}\,i)/2)=\boldsymbol{Q}(\sqrt{2},i),$$

$\sigma_3\zeta_8=\zeta_8^3=\zeta_8^2\zeta_8=i\zeta_8=(-\sqrt{2}+\sqrt{2}\,i)/2$，$\sigma_5\zeta_8=(-\sqrt{2}-\sqrt{2}\,i)/2$，$\sigma_{-1}\zeta_8=(\sqrt{2}-\sqrt{2}\,i)/2$. 故$\sigma_{-1}$，$\sigma_5$，$\sigma_3$分别固定$\sqrt{2}$，$i$，$\sqrt{2}\,i$. 从而$\boldsymbol{Q}(\sqrt{2})$，$\boldsymbol{Q}(i)$，$\boldsymbol{Q}(\sqrt{2}\,i)$分别对应特征子群$\langle\rho\rangle$，$\langle\psi\rangle$，$\langle\psi\rho\rangle$.



任一 Abel 数域 K 必含于某分圆域 $\mathbf{Q}(\zeta_m)$ 中(Kronecker—Weber 定理，见下章)，故总可用 D—特征群刻画. 以下用特征群刻画素理想分解. 设

$$m = \prod_p p^s,$$

于是相应有直和分解

$$G_m = (\mathbf{Z}/m\mathbf{Z})^* = \coprod (\mathbf{Z}/p^s\mathbf{Z})^*,$$

$$\hat{G}_m = \prod_p \hat{G}_{p^s},$$

$$\chi = \prod_p \chi_p.$$

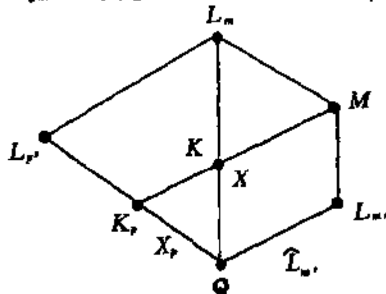
其中 χ_p 是模 p^s 特征，称为 χ 的 p—分量. 设 X 是 $\hat{G}_m$ 的子群，记

$$X_p = \{\chi_p \mid \chi \in X\}.$$

定理 1 设 $X = \hat{K}$ 是 Abel 域 K 的特征群，则素数 p 在 K 的分歧指数为

$$e_p(K) = \#(X_p).$$

证明 设 $m = \underset{\chi \in X}{\mathrm{Lcm}}\{f_\chi\}$，则 $K \subset L_m$. 设 $m = p^s m'$，$p \nmid m'$，记 $M = KL_{m'} = K(\zeta_{m'})$，于是 $\hat{M} = \langle X, \hat{L}_{m'} \rangle = X_p \times \hat{L}_{m'}$，其中 $\times$



表示直积．记 X_p 对应的子域为 K_p，则 $M=K_pL_{m'}$．由于 p 在 $L_{m'}$ 不分歧，故 $e_p(K)=e_p(M)=e_p(K_p)=[K_p:\boldsymbol{Q}]=\#(X_p)$．定理证毕． □

在定理 1 中，$e_p(K)=1$ 意味着 $(X_p)=0$，即 $\chi\in X$ 的 p-分量均是平凡的，故有

系 1 p 在 K 非分歧 $\Leftrightarrow X(p)\neq 0 \quad (\forall\ \chi\in\hat{K})$

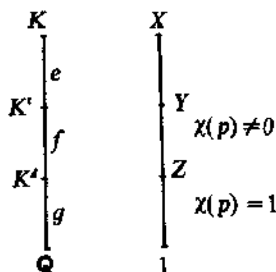
$$\Leftrightarrow p\nmid f_\chi \quad (\forall\ \chi\in\hat{K}).$$

定理 2 设 $X=\hat{K}$ 是 Abel 域 K 的特征群，令 $Y=\{\chi\in \boldsymbol{X}\mid\chi(p)\neq 0\}$，$Z=\{\chi\in X\mid\chi(p)=1\}$，则

(1) $X/Y\cong T_p$ (p 的惯性群)．

(2) $X/Z\cong D_p$ (p 的分解群)．

(3) $Y/Z\cong D_p/T_p$．



证明 Y 对应的子域 K_Y 是 p 在 K 的最大非分歧子域，故 $K_Y=K^t$ 为惯性域．从而 $T_p=G(K/K_Y)=X/Y$．

现在 $\hat{K}_Y=Y$，设 $m=\mathrm{Lcm}\{f_\chi\}$ $(\chi\in Y)$，则 $K_Y\subset L_m=\boldsymbol{Q}(\zeta_m)$，$p\nmid m$，$p$ 在 L_m 的 Frobenius 自同构 $\sigma_p=p\in(\mathbf{Z}/m\mathbf{Z})^*=G_m$．而 p 在 K_Y 的 Frobenius 自同构 σ_p' 是 σ_p 在 K_Y 的限制．若 $\chi\in Y$，则 χ 在 $\mathrm{Gal}(L_m/K_Y)$（限制映射的核）上作用平凡，故 $\chi(\sigma_{p'})=\chi(\sigma_p)$．特别 $x(\sigma'_p)=1\Leftrightarrow\chi(p)=1$ 故 $Z=\langle\sigma_p'\rangle^\perp$（对于配对 $G(K_Y)\times Y$

$\longrightarrow C^*$). 故

$$Y/Z \cong \langle \sigma_p' \rangle^{\wedge} \cong \langle \sigma_p' \rangle.$$

特别知剩余类次数 $f \triangleq \# \langle \sigma_p' \rangle = (Y : Z)$. 因 Frobenius 自同构 σ_p' 的固定子域是 p 的分裂域 K^d, 故由 $Z = (\sigma_p')^{\perp}$ 知 $Z = \hat{K}^d$, $g = (Z : 1)$, 这也说明 $X/Z \cong D_p$. □

§8.3 Dirichlet 级数

数论中常涉及如下类型的级数, 称为 Dirichlet 级数, 或简称为 D-级数:

$$f = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

其中 s 是复变数, $\{a_n\}$ 是复数序列, 常记

$$s = \sigma + i\tau \qquad (\sigma, \tau \in \mathbf{R}).$$

定理 1 (D-级数的有敛性) 若 D-级数 $f = \Sigma a_n/n^s$ 对 $s = s_0$ 收敛, 则在区域 $\mathrm{Re}(s) > \sigma_0 = \mathrm{Re}(s_0)$ 内收敛, 且在此区域中任一紧集上一致收敛(其中 $\mathrm{Re}(s)$ 表示 s 的实部).

证 先回忆部分求和法. 设 $A_n = a_1 + \cdots + a_n$, $B_n = b_1 + \cdots + b_n$, 则

$$\sum_{n=1}^{N} a_n b_n = A_N B_N + \sum_{n=1}^{N-1} A_n (b_n - b_{n+1}).$$

所给级数 f 可写为

$$f = \sum \frac{a_n}{n^{s_0}} \frac{1}{n^{s-s_0}}$$

记 $P_n(s_0) = \sum_{k=1}^{n} a_k/k^{s_0}$，则 f 的尾段

$$f_{m,n} = \sum_{k=m+1}^{n} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}} =$$

$$= \frac{P_n(s_0)}{n^{s-s_0}} - \frac{P_m(s_0)}{m^{s-s_0}} + \sum_{k=m}^{n-1} P_k(s_0) B,$$

其中 $B = \frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} = (s-s_0)\int_k^{k+1} \frac{dx}{x^{s-s_0-1}}$.

由题设知 $|P_n(s_0)| < P$(常数). $\mathrm{Re}(s) = \sigma \geqslant \sigma_o + \delta(\delta > 0)$,

$|s-s_0| < C$(常数), $|x^{s-s_0}| = |x|^{\sigma-\sigma_o} \geqslant |x|^{\delta}$,故

$$\left|\sum_{k=m}^{n-1} P_k(s_o) B\right| \leqslant P\sum_{m}^{n-1}|B| \leqslant PC\sum_{m}^{n-1}\int_k^{k+1}\frac{dx}{x^{\delta+1}}$$

$$\leqslant PC\delta^{-1}(\frac{1}{m^{\delta}} - \frac{1}{n^{\delta}}) \leqslant PC^{\delta-1}/m^{\delta} \longrightarrow 0 (当\ m \to \infty).$$

定理证毕. □

由此可知，对于 D-级数 f，总存在实数 σ_o(称为**收敛横坐标**)，使当 $\mathrm{Re}(s) > \sigma_o$ 时 f 收敛，当 $\mathrm{Re}(s) < \sigma_o$ 时 f 不收敛.

定理 2 若存在常数 M 和 $\sigma_1 > 0$ 使

$$|A_n| = |a_1 + \cdots + a_n| \leqslant Mn^{\sigma_1} \quad (\forall\ n),$$

则 $f = \Sigma a_n/n^s$ 的收敛横坐标 $\sigma_0 \leqslant \sigma_1$.

证明 $f_{m,n} = \sum_{k=m+1}^{n} a_k \frac{1}{k^s} = \frac{A_n}{n^s} - \frac{A_m}{m^s} + \sum_{k=m}^{n-1} A_k B_1$,

其中

$$B_1 = \frac{1}{k^s} - \frac{1}{(k+1)^s} = s\int_k^{k+1} \frac{dx}{x^{s+1}}.$$

设 $\mathrm{Re}(s) = \sigma = \sigma_1 + \delta(\delta > 0)$. 如同定理 1 证明可知

$$\left|\sum_{k=m}^{n-1} A_k B_k\right| \leqslant M\sum_{m}^{n-1} k^{\sigma_1}|B_k| \leqslant M\sum_{m}^{n-1} k^{\sigma_1}|s|\int_k^{k+1}\frac{dx}{x^{s+1}}$$

$$\leqslant M|s|\sum_{m}^{n-1}\int_k^{k+1}\frac{dx}{x^{\delta+1}} \leqslant M|s|\delta^{-1}/m^{\delta} \to 0.$$

再由 $|A_n/n^s|\leqslant M/n^{\delta}\to 0$，即得所欲证. □

设

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s},$$

这称为 Riemann Zeta 函数，因 $|A_n|=n^1$，由定理 2 可知 $\zeta(s)$的收敛横坐标 $\sigma_0\leqslant 1$. 对实数 $s>1$，用积分逼近 $\zeta(s)$有

$$\frac{1}{s-1}\leqslant\int_1^{\infty}\frac{dx}{x^s}\leqslant\zeta(s)\leqslant 1+\frac{1}{s-1},$$

故

$$1\leqslant(s-1)\zeta(s)\leqslant s.$$

这说明，如果 $\zeta(s)$可解析开拓到 $\mathrm{Re}(s)<1$(除个别奇点之外)，则 $s=1$ 是其 1 阶极点，留数为 1，即 $\zeta(s)=1/(s-1)+a^2/(s-1)^2+\cdots$.

定理 3 当 $\mathrm{Re}(s)>0$ 且 $s\neq 1$ 时，$\zeta(s)$解析．而 $s=1$ 是$\zeta(s)$的 1 阶极点，留数为 1.

证明 令

$$\zeta_2(s) = 1-\frac{1}{2^s}+\frac{1}{3^s}-\cdots = \sum a_n/n^s,$$

则 $A_n = \sum_{1}^{n} a_k = 0$ 或 1，由定理 2 知 $\zeta_2(s)$ 对于 $\mathrm{R_e}(s)>0$ 解析. 而

$$\zeta(s)=\zeta_2(s)+\zeta(s)/2^{s-1}. \ (\mathrm{Re}(s)>1),$$

即

$$\zeta_2(s)=(1-1/2^{s-1})\zeta(s).$$

这就将 $\zeta(s)$ 解析开拓到了 $\mathrm{Re}(s)>0$，再证除 $s=1$ 之外无极点. 即要证 $1=1/2^{s-1}$ 时，即 $s=2\pi in/\log 2+1(n\in\mathbf{Z})$ 时，s 不是 $\zeta(s)$ 的极点. 但若令

$$\zeta_3(s)=1+\frac{1}{2^s}-\frac{2}{3^s}+\frac{1}{4^s}+\cdots\cdots$$

则同上可知 $\zeta_3(s)=(1-1/3^{s-1})\zeta(s)$，于是 $\zeta(s)$ 的可能极点只能是 $s=2\pi im/\log 3+1(m\in\mathbf{Z})$，从而需要 $3^n=2^m$，此不可能. □

定理 4 设有复数 ρ，常数 $C>0$ 和 $0\leqslant\sigma_1<1$ 使

$$A_n=a_1+\cdots+a_n=n\rho+O(n^{\sigma_1}),$$

即

$$|A_n-n\rho|\leqslant Cn^{\sigma_1} \qquad (\forall\ n>0),$$

则 $f=\sum a_n/n^s$ 可解析开拓至 $\mathrm{Re}(s)>\sigma_1$，只在 $s=1$ 为单极点且留数为 ρ.

证明 $f(s)-\rho\zeta(s)$ 的系数部分和为 $A_n-n\rho$，故由定理 2 知 $f(s)-\rho\zeta(s)$ 在 $\mathrm{Re}(s)>\sigma_1$ 收敛且解析. 再由定理 3 即得. □

§8.4 Zeta 函数和 L-函数

设 K 为 n 次数域，记 $N(I)=N_{K/\mathbf{Q}}(I)$. K 的 (Dedekind) Zeta 函数定义为

$$\zeta_K(s) = \sum_I \frac{1}{NI^s},$$

其中 I 过 K 的整理想.

定理 1 设 $\sigma=Re(s)>1$，$\wp$ 过 K 的非 0 素理想，则有：

(1) $\sum_{\wp}\frac{1}{N\wp^{\sigma}}$ 收敛.

(2) $\prod_{\wp}(1-N\wp^{-s})^{-1}$ 绝对收敛且在紧子集上一致收敛.

(3) $\zeta_K(s)=\sum_I NI^{-s}$ 绝对收敛且在紧子集上一致收敛.

(4) $\zeta_K(s)=\prod_{\wp}(1-N\wp^{-s})^{-1}$，特别知当 $\mathrm{Re}(s)>1$ 时 $\zeta_K(s)\neq 0$.

证明 (1) $\sum_{\wp} N\wp^{-\sigma}=\sum_{p\in Z}\sum_{\wp|p}N\wp^{-\sigma}\leqslant n\sum_p p^{-\sigma}\leqslant n\sum_{m=1}^{\infty}m^{-\sigma}$，此为收敛.

(2) 固定 $\sigma_0>1$，在 $\sigma\geqslant\sigma_0$ 区域考虑此乘积. 由 $N\wp\geqslant 2$ 知有

$$\begin{aligned}\log(1-|N\wp^{-s}|)^{-1}&=\sum_{m=1}^{\infty}N\wp^{-\sigma m}/m\leqslant\sum_{m=1}^{\infty}N\wp^{-\sigma m}\\&=N\wp^{-\sigma}/(1-N\wp^{-\sigma})\\&\leqslant N\wp^{-\sigma_0}/(1-N\wp^{-\sigma_0})\leqslant 2N\wp^{-\sigma_0}\end{aligned}$$

由(1)知 $\sum_{\wp}N\wp^{-\sigma_0}$ 收敛，故知 $\sum_{\wp}\log(1-|N\wp^{-s}|)^{-1}$ 当 $\sigma\geqslant\sigma_0$ 时一致收敛. 从而知(2)中乘积如所欲证.

(3) 考虑有限积

$$\prod_{N\wp\leqslant t}(1-N\wp^{-s})^{-1}=\prod_{N\wp\leqslant t}(1+N\wp^{-s}+N\wp^{-2s}+\cdots)$$

$$-\Sigma' NI^{-s},$$

其中Σ'表示对素理想因子$\wp$满足$N\wp\leqslant t$的整理想I求和. 故知

$$\prod_{N\wp\leqslant t}(1-N\wp^{-s})^{-1}=\sum_{NI\leqslant t}NI^{-s}+\sum_{NI>t}NI^{-s}.$$

固定$\sigma_0>1$有

$$\sum_{NI\leqslant t}NI^{-\sigma_0}<\prod_{N\wp\leqslant t}(1-N\wp^{-\sigma_0})^{-1}<\prod_{\wp}(1-N\wp^{-\sigma_0})^{-1}.$$

于是知$\sum NI^{-s}$对$\mathrm{Re}(s)>1$绝对收敛.

上述也说明

$$\left|\prod_{N\wp\leqslant t}(1-N\wp^{-s})^{-1}-\sum_{NI\leqslant t}NI^{-s}\right|\leqslant\sum_{NI>t}NI^{-\sigma}.$$

当$\sigma\geqslant\sigma_0>1$时，右方有上界$\sum\limits_{NI>t}NI^{-\sigma_0}\longrightarrow 0(t\to\infty)$. 这证明了(3) 中级数当$\mathrm{Re}(s)\geqslant\sigma_0$时一致收敛，也证明了(4). □

设B是K的一个理想类，B的Zeta函数定义为

$$\zeta(s,B)=\sum_{I\in B}NI^{-s}$$

其中I仅取整理想. 显然$\zeta_K(s)=\sum\limits_{B}\zeta(s,B)$.

定理2 (1)$\zeta(s,B)$在$\mathrm{Re}(s)>1-\frac{1}{n}$且$s\neq 1$时解析，在$s=1$为单极点，留数为

$$\rho_K=2^{r_1}(2\pi)^{r_2}R_K/w\sqrt{d_K},$$

(2) 上述对$\zeta_K(s)$也成立，但留数为$h_K\rho_K$.

(3) K含无限多素理想$\wp$使$f(\wp)=1$.

上述r_1和$2r_2$是K到$\boldsymbol{C}$的实和虚嵌入个数，R_K为K的正规子

(§6.4 习题 1)，w 是 K 的单位根群的阶，d_K 为 K 的判别式绝对值，h_K 为 K 的类数，$f(\wp)=f(\wp\mid p)$ 为 $\wp$ 的剩余类次数，$(p)=\wp\cap\mathbf{Z}$.

证明 (1) 记 a_k 为使 $Na=k$ 的 $a\in B$ 的个数，则 $\zeta(s,B)=\sum\limits_{k\geqslant 1}a_k/k^s$. 记 $A_m=a_1+\cdots+a_m=$ (类 B 中范数 $\leqslant m$ 的整理想个数). 用第六章方法(见[La]P.132)可算得

$$A_m=j(B,m)=\rho_K m+O(m^{1-1/n}),$$

再由上节定理 4 即得(1).

(2) 由 $\zeta_K(s)=\sum\limits_{B}\zeta(s,B)$ 即知.

(3) 在区域 $\{z:|z|<1\}$ 取对数分支使 $\log 1=0$，则此分支为 $\log(1-z)=-\sum\limits_{v=1}^{\infty}v^{-1}z^v$. 用此分支，当实数 $\sigma>1$ 时有

$$\begin{aligned}\log\zeta_K(\sigma)&=\sum_{\wp}\log(1-N\wp^{-\sigma})^{-1}\\&=\sum_{\wp}\sum_{v=1}^{\infty}(vN\wp^{\sigma v})^{-1}\\&=\sum_{\wp}N\wp^{-\sigma}+\sum_{\wp}\sum_{v\geqslant 2}(vN\wp^{\sigma v})^{-1},\end{aligned}$$

第二个和式(若以 s 代 σ)在 $\mathrm{Re}(s)>\sigma_0>\frac{1}{2}$ 的任一区域中收敛，这是由于

$$\begin{aligned}&\sum_{\wp}\sum_{v\geqslant 2}|vN\wp^{sv}|^{-1}<\frac{1}{2}\sum_{\wp}\sum_{v\geqslant 2}|N\wp^{-sv}|\\&=\frac{1}{2}\sum_{\wp}|N\wp^{-2s}|(1-|N\wp^{-s}|)^{-1}\\&\leqslant\frac{1}{2}(1-2^{-\sigma_0})^{-1}\sum_{\wp}N\wp^{-2\sigma_0},\end{aligned}$$

且最后的和式有上界 $n\sum\limits_{m=1}^{\infty}m^{-2\sigma_0}$，它当 $\sigma_0>\frac{1}{2}$ 时收敛. 故若 $\sigma\to$

1^+，则 $\sum_{\wp} N\wp^{-\sigma} \to \infty$. 又因

$$\sum_{\wp} N\wp^{-\sigma} = \sum_{f(\wp)=1} N\wp^{-\sigma} + \sum_{f(\wp)\geqslant 2} N\wp^{-\sigma},$$

最右方的和式在 $\sigma = 1$ 收敛，故 $\sum_{f(\wp)=1} N\wp^{-1}$ 发散. □

定义 1 设 χ 为本原 Dirichlet 特征. 下式称为 χ 的 Dirichlet L-函数：

$$L(s, \chi) = \sum_{v=1}^{\infty} \frac{\chi(v)}{v^s}.$$

定理3 设 $\chi \neq 1$，则 $L(s, \chi)$ 在区域 $\mathrm{Re}(s) > 0$ 绝对收敛，且在其内紧集中一致收敛. 而当 $\mathrm{Re}(s) > 1$ 时有欧拉乘积

$$L(s, \chi) = \prod_{p} \frac{1}{1 - \chi(p)/p^s}$$

证明 对任一 Abel 群 G 及其特征群 $\hat{G}$，固定 $\chi \in \hat{G}$. 显然有

$$\sum_{g \in G} \chi(g) = \# G \text{ 或 } 0(\text{依 } \chi = 1 \text{ 或否}),$$

这是由于当 $\chi \neq 1$ 时，取 $a \in G$ 使 $\chi(a) \neq 1$ 则有

$$\sum_{g} \chi(g) = \sum_{g} \chi(ag) = \chi(a) \sum_{g} \chi(g).$$

故知 L − 函数相应的系数部分和 $A_m = \sum_{1}^{m} \chi(v)$ 有界，即得第一个结论. 其余证明与定理 1 相同. □

定理 4 设分圆域 $K = Q(\zeta_m)$，则

$$\zeta_K(s) = \prod_{\chi} L(s, \chi),$$

其中 χ 过所有满足 $f_\chi|m$ 的本原 Dirichlet 特征.

证明 只需对实数 $s>1$ 证明. 此时 $\zeta_K(s)=\prod\limits_{\wp}(1-N\wp^{-s})^{-1}$, $\prod\limits_{\chi}L(s,\chi)=\prod\limits_{\chi}\prod\limits_{p}(1-\chi(p)p^{-s})^{-1})$, 故只需证

$$\prod_{\wp,p}(1-N\wp^{-s})=\prod_{\chi}(1-\chi(p)p^{-s}\qquad(*)$$

对任一素数 p 成立. 设 $m=p^rm'(p\nmid m',r\geqslant 0)$. 于是 p 在 K 中分解为 $(p)=(\wp_1\cdots\wp_g)^e$, $N\wp_i=p^f$, $e=\varphi(p^r)$, f 是使 $p^f\equiv 1(\mathrm{mod}m')$ 最小正整数, $efg=\varphi(m)$. 故 $(*)$ 式左方为 $(1-p^{-fs})^g$, 右方为 $\prod\limits_{f_\chi|m'}(1-\chi(p)p^{-s})$. 满足 $f_\chi|m'$ 的 χ 全体即为 $\hat{G}_{m'}$(即模 m' 特征全体). 当 χ 过 $\hat{G}_{m'}$ 时, $\chi(p)$ 过 f 次单位根群 W 共 $\varphi(m')/f=g$ 次, 故 $(*)$ 式右方为 $\prod\limits_{w\in W}(1-wp^{-s})^g=(1-p^{-fs})^g$. □

定理 5 记 h_K 为 $K=\boldsymbol{Q}(\zeta_m)$ 的类数, 则

$$\rho_Kh_K=\prod_{1\neq\chi\in\hat{G}_m}L(1,\chi),$$

特别可知对任意 χ 有

$$L(1,\chi)\neq 0.$$

证明 在 $\zeta_k(s)=\prod\limits_{\chi}L(s,\chi)$ 两边令 $s=1$(先乘以 $s-1$), 因 $L(s,1)=\zeta(s)$ 留数为 1, $\zeta_K(s)$ 留数为 ρ_Kh_K, 其余 $L(s,\chi)$ 解析(在 $s=1$, 当 $\chi\neq 1$), 即得结论.

定理 6 (Dirichlet 算术序列定理) 算术序列 $m+nd$ (n

$= 1, 2, 3, \cdots$) 中含无限多素数，这里 m 与 d 为互素正整数.

证明 设 $\chi \in \hat{G}_m = (\mathbf{Z}/m\mathbf{Z})^{\wedge}$，则 $L(s, \chi) = \sum_p \log(1 - \chi(p)p^{-s})^{-1} = \sum_{p, n} \chi(p)^n / np^{ns} \sim \sum_p \chi(p)p^{-s}$（其中 $f(s) \sim g(s)$ 指 $f(s) - g(s)$ 在 $s = 1$ 解析）. 于是

$$\log L(s, \chi) \sim \sum_{p \nmid m} \chi(p)p^{-s} = \sum_{C \in G_m} \chi(C) \sum_{p \in C} p^{-s}.$$

固定一剩余类 $A \in G_m$，对右方等式乘以 $\chi(A^{-1}$，并对 $\chi \in \hat{G}_m$ 求和，则得

$$\begin{aligned}\sum_\chi \chi(A^{-1}) \log L(s, \chi) &\sim \sum_{\chi, C} (A^{-1}C) \sum_{p \in C} p^{-s} \\ &= \sum_C \sum_\chi \chi(A^{-1}C) \sum_{p \in C} p^{-s}.\end{aligned}$$

$$\sum_\chi \chi(A^{-1}C) = 0 \text{ 或 } \varphi(m) (\text{当 } A \neq C \text{ 与否}).$$

故

$$\sum_\chi \chi(A^{-1}) \log L(s, \chi) \sim \varphi(m) \sum_{p \in A} p^{-s}.$$

当 $\chi \neq 1$ 时，$L(1, \chi) \neq 0$，故知

$$\log \zeta(s) \sim \varphi(m) \sum_{p \in A} p^{-s}. \qquad \square$$

设 $X = \hat{K}$ 是 Abel 数域 K 的特征群，令

$$m = \operatorname*{lcm}_{\chi \in \hat{K}} \{f_\chi\},$$

则 $K \subset L_m = \boldsymbol{Q}(\zeta_m)$. 此 m 称为 K（和 X）的**导子**（即使 $K \subset \boldsymbol{Q}(\zeta_m)$ 的最小正整数）.

定理 7 设 K 为 Abel 数域，则

$$\zeta_K(s) = \prod_{\chi \in \hat{K}} L(s, \chi).$$

证明 如同定理 4 一样，只需证明对每个素数 p 有

$$\prod_{\wp | p} (1 - N\wp^{-s}) = \prod_{\chi \in \hat{K}} (1 - \chi(p) p^{-s}). \qquad (*)$$

设 p 在 K 分解为 $(p) = (\wp_1 \cdots \wp_g)^e$，$f(\wp_i | p) = f$，$N\wp_i = p^f$. 于是 $(*)$ 左边为 $(1 - p^{-fs})^g$. 右方可忽略使 $\chi(p) = 0$ 的 χ. 由 §8.2 定理 2 知，Y/Z 是 f 阶循环群，其中 $Y = \{\chi \in X = \hat{K} | \chi(p) \neq 0\}$，$Z = \{\chi | \chi(p) = 1\}$. 当 χ 过 Y/Z 的一个陪集代表元系时，$\chi(p)$ 过 f 次单位根群，每个陪集有 g 个元素，故 $(*)$ 式右方为

$$\prod_{k=0}^{f-1} (1 - \zeta_f^k p^{-s})^g = (1 - p^{-fs})^g. \qquad \square$$

以上已将 $\zeta_K(s)$ 和 $L(s, \chi)$ 解析开拓到复半平面 $\mathrm{Re}(s) > 0$ ($\zeta_K(s)$ 有单极点 $s = 1$). 事实上，这两种函数可解析开拓至全复平面，并且各满足一个"函数方程"，此类函数方程将 s 点上值对应到 $1 - s$ 点上的值，建立了以直线 $\mathrm{Re}(s) = \frac{1}{2}$ 为"对称轴"的某种意义上的"对称". 以下叙述这一理论及应用，证明细节可见[La]. 记 $f = f(\chi)$ 为 χ 的导子，并记

$$\delta = \delta(\chi) = 0 \text{ 或 } 1 (\text{依 } \chi(-1) = 1 \text{ 或 } -1).$$

$$\tau(\chi) = \sum_{a=1}^{f} \chi(a) e^{2\pi i a/f}, \qquad (\text{Gauss 和}, \tau(1) = 1)$$

$$\Lambda(s, \chi) = (f/\pi)^{s/2} \Gamma((s + \delta)/2) L(s, \chi),$$

其中 $\Gamma(s)=s^{-1}\prod_{n=1}^{\infty}(1+1/n)^{s}(1+s/n)^{-1}=\int_{0}^{\infty}e^{-t}t^{s-1}dt$ 为 Γ-函数(后一等式是当 s 为实数). Γ-函数满足 $\Gamma(s+1)=s\Gamma(s)$. 且可表为

$$\frac{1}{\Gamma(s)}=se^{cs}\prod_{n=1}^{\infty}(1+\frac{s}{n})e^{-s/n}$$

($c=0.577\cdots$ 为欧拉常数). 在复平面上, $\Gamma(s)$ 在 $s=0,-1,-2,\cdots$ 具有一阶极点, 在其余点均解析.

定理 8 $\Lambda(s,\chi)$ 可被解析开拓为全复平面上的半纯函数, 且满足函数方程

$$\Lambda(s,\chi)=(\frac{\tau(\chi)}{\sqrt{f}i^{\delta}})\Lambda(1-s,\overline{\chi}).$$

特别知, 当 $\chi\neq 1$ 时, $L(s,\chi)$ 是全复平面上的全纯函数. 而当 $\chi=1$ 时, $L(s,1)=\zeta(s)$ 只有唯一的极点 $s=1$(这里 $\overline{\chi}(a)=\overline{\chi(a)}$).

$W_{\chi}=\tau(\chi)/\sqrt{f}i^{\delta}$ 常称为根数. 函数方程也可写为

$$L(s,\chi)$$
$$=W_{\chi}(f/\pi)^{(1-2s)/2}\Gamma(\frac{(1-s+\delta)}{2})\Gamma(\frac{(s+\delta)}{2})^{-1}L(1-s,\overline{\chi}).$$

注意 $\Gamma(s)$ 总非 0. 当 $\chi\neq 1$ 时, 我们已证过 $L(s,\chi)$ 在 $\mathrm{Re}(s)>0$ 时解析. 故由函数方程即可知道, $L(s,\chi)$ 在 $\mathrm{Re}(s)\leqslant 0$ 时若有极点, 只能来自因子 $\Gamma(\frac{1-s+\delta}{2})$ 的极点, 即 $\Gamma(z)$ 在 $\mathrm{Re}(z)\geqslant\frac{1}{2}$ 的极点, 此不可能. 再看 $\chi=1$ 时, 函数方程化为

$$\Gamma(\frac{s}{2})\pi^{-s/2}\zeta(s)=\Gamma(\frac{1-s}{2})\pi^{-(1-s)/2}\zeta(1-s).$$

由此可知$s=-2,-4,-6,\cdots,-2n,\cdots$为$\zeta(s)$的零点，这称为平凡零点. 还可证明，$\zeta(s)$在负奇整数处的值$\zeta(1-2n)$均为有理数.

对任意n次数域K，Dedekind Zeta 函数$\zeta_K(s)$也可开拓为全复平面上的半纯函数，唯一的极点为$s=1$. 当$\mathrm{Re}(s)\geqslant 1$时，$\zeta_K(s)$没有零点. 当$\mathrm{Re}(s)\leqslant 0$时，在$-1,-3,-5,\cdots$有$r_2$阶零点；在$-2,-4,-6,\cdots$有$r_1+r_2$阶零点. 其它的零点都在带状区$0<\mathrm{Re}(s)<1$之内(称为非平凡零点)，实际上确实有无限多个非平凡零点. 猜想非平凡零点都在直线$\mathrm{Re}(s)=\frac{1}{2}$上(Riemann 猜想). 记

$$Z_K(s)=\left(\frac{\sqrt{d_K}}{2^{r_2}\pi^{n/2}}\right)^s\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta_K(s),$$

则有函数方程(Hecke, 1917)：

$$Z_K(s)=Z_K(1-s).$$

当K/k为 Galois 扩张时，$\zeta_K(s)/\zeta_k(s)$为整函数(R. Brauer, 1947).

§8.5 类数公式

继续上节讨论，仍设K为n次数域，当K为 Abel 域时，有$\zeta_K(s)=\prod\limits_{\chi\in\hat{K}}L(s,\chi)$. 将两边的函数方程相比较可知.

$$(d_K\Pi f_\chi^{-1})^{s/2}=\prod_\chi(\chi(-1)f_\chi)^{1/2}\tau(\chi)^{-1}(d_k\Pi f_\chi^{-1})^{(1-s)/2}$$

对所有s成立，从而两边均等于 1. 即得：

定理 1 设 K 为 n 次 Abel 数域.

(1)(导子一判别式公式). $K/\mathbf{Q}$ 的判别式 $D(K)=(-1)^{r_2}d_K$ 为:

$$D(K)=(-1)^{r_2}\prod_{\chi\in\hat{K}}f_\chi.$$

(2) $$\prod_{\chi\in\hat{K}}\tau(\chi)=\prod_{\chi\in\hat{K}}\sqrt{\chi(-1)f_\chi}.$$

$$=\begin{cases}\sqrt{d_K}, & \text{若 } K \text{ 是(全)实域},\\ i^{n/2}\sqrt{d_K}, & \text{若 } K \text{ 是虚域}.\end{cases}$$

证明 $D(K)$ 的符号为 $(-1)^{r_2}$(见 §1.5). 因 K 为 Galois 域, 故只能 $r_1=0$ 或 $r_2=0$. 前一情形 K 为(全)实域, $\chi(-1)=1$. 后一情形 K 为虚域, 使 $\chi(-1)=1$ 的实特征 χ 形成指数为 2 的子群. 故有 $n/2$ 个 $\chi\in\hat{K}$ 使 $\chi(-1)=-1$. □

定理1中当 K 为二次域时, 若 χ 是模 p 的唯一的二阶特征, 则 $K=\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$(见 §7. 4), 故

$\tau(\chi)=\sqrt{p}$ 或 $i\sqrt{p}$(依 $p\equiv 1$ 或 $3(\bmod 4)$).

在 $\zeta_K(s)=\zeta(s)\prod_{\chi\neq 1}L(s,\chi)$ 两边乘以 $(s-1)$, 再令 $s\to 1$. 由于 $\zeta_K(s)$ 在 $s=1$ 的留数为 $\rho_K h_K$, $\zeta(s)$ 的留数为 1, 其余 $L(s,\chi)$ 均解析且 $L(1,\chi)\neq 0$, 故得

$$\rho_K h_K=\prod_{\chi\neq 1}L(1,\chi).$$

如果能给出 $L(1,\chi)$ 一个较简单的表达, 由此就可得到求类数 h_K 的公式(类数公式). 注意 $\rho_K=2^{r_1}(2\pi)^{r_2}R_K/w\sqrt{d}_K$. 因为 K 为 Galois 域(实为 Abel 域), 故 $r_1=0$ 或 $r_2=0$. 于是有

引理 1

$$R_K h_K = \begin{cases} d_K^{1/2} 2^{1-r} \prod\limits_{\chi \neq 1} L(1, \chi), & \text{若 } K \text{ 为实域}. \\ w d_K^{1/2} (2\pi)^{-n/2} \prod\limits_{\chi \neq 1} L(1, \chi), & \text{若 } K \text{ 为虚域}. \end{cases}$$

现设 $\chi \neq 1$ 为本原特征，$f = f_\chi$ 为其导子，$\zeta = \zeta_f$.

定理 2 (1) 若 χ 为奇特征，则

$$L(1, \chi) = \frac{\pi i \tau(\chi)}{f^2} \sum_{a=1}^{f} \overline{\chi}(a) a.$$

(2) 若 χ 为偶特征，则

$$L(1, \chi) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log |1 - \zeta^a|$$

$$= -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log \sin \frac{\pi a}{f}.$$

证明 $L(s, \chi) = \sum\limits_{v=1}^{\infty} \chi(v) v^{-s} = \sum\limits_{(b, f)=1} \chi(b) \sum\limits_{v \equiv b(f)} v^{-s}$（当 $\mathrm{Re}(s) > 1$）. 最后和式可视为 D- 级数 $\Sigma c_v v^{-s}$，其中 $c_v = 1$ 或 0（依 $v \equiv b(\mathrm{mod} f)$ 与否），而 $\sum\limits_{a=1}^{f} \zeta^{ra} = f$ 或 0（依 $r \equiv 0(\mathrm{mod} f)$ 与否），故 $c_v = f^{-1} \sum\limits_{a=1}^{f} \zeta^{(b-v)a}$. 故

$$L(s, \chi) = \sum_{(b, f)=1} \chi(b) \sum_{v=1}^{\infty} f^{-1} \sum_{a=0}^{f} \zeta^{(b-v)a} v^{-s}$$

$$= f^{-1} \sum_{a} \left(\sum_{b} \chi(b) \zeta^{ab} \right) \sum_{v=1}^{\infty} \zeta^{-va} v^{-s}$$

$$= f^{-1}\sum_{a=1}^{f}\tau_a(\chi)\sum_{v=1}^{\infty}\zeta^{-va}v^{-s}.$$

其中

$$\tau_a(\chi) = \sum_{(b,f)=1}\chi(b)\zeta^{ab} \qquad (\text{Gauss 和}).$$

显然 $\tau_0(\chi) = 0$. 当 $a \neq 0$ 时，部分和 $\sum_{v=1}^{n}\zeta^{-va}$ 有界. 故当 $\mathrm{Re}(s) > 0$ 时，$\Sigma\zeta^{-va}v^{-s}$ 收敛，从而得

$$L(1,\chi) = f^{-1}\sum_{a=1}^{f}\tau_a(\chi)\sum_{v=1}^{\infty}\zeta^{-va}/v.$$

而 $\sum_{v=1}^{\infty}z^v/v = -\log(1-z)$（在闭单位圆盘，$z \neq 1$），这里分支 $\log(1-z)$ 当 $z = 0$ 时取值为 0. 即得

$$L(1,\chi) = -f^{-1}\sum_{a=1}^{f}\tau_a(\chi)\log(1-\zeta^{-a}).$$

我们留在下面引理证明：当 $(a,f) \neq 1$ 时，$\tau_a(\chi) = 0$. 由 $\tau_a(\chi) = \bar{\chi}(a)\tau(\chi)$ 知，上述分式可改写为

$$L(1,\chi) = (-\tau(\chi)/f)\sum_{a}\bar{\chi}(a)\log(1-\zeta^{-a}).$$

其中 a 可取遍模 f 的任一剩余系或缩系. 再由

$$\begin{aligned}1-\zeta^{-a} &= 1-e^{-2\pi ia/f}\\ &= \exp(-i\pi a/f)(\exp(i\pi a/f)-\exp(-i\pi a/f))\\ &= 2i\exp(-i\pi a/f)\sin(\pi a/f)\\ &= 2\exp(i\pi/2-i\pi a/f)\sin(\pi a/f).\end{aligned}$$

当 $0 < a < f$ 时，$(\pi/2-\pi a/f) \in (-\pi/2,\pi/2)$，故

$$\log(1-\zeta^{-a}) = \log(2\sin(\pi a/f)) + i\pi(1/2-a/f),$$

$$\log(1-\zeta^{a}) = \log(2\sin(\pi a/f)) - i\pi(1/2-a/f).$$

（后者由取共轭得）. 若 χ 为奇特征，在如下定义的 S 中易 a 为 $-a$ 并相加得

$$S:=\sum_{a=1}^{f-1}\overline{\chi}(a)\log(1-\zeta^{-a})=-\sum_{a=1}^{f-1}\overline{\chi}(a)\log(1-\zeta^{a}),$$

$$\begin{aligned}2S&=\sum_{a}\overline{\chi}(a)(\log(1-\zeta^{-a})-\log(1-\zeta^{a}))\\&=2\sum_{a}\overline{\chi}(a)i\pi(1/2-a/f).\end{aligned}$$

由 $\sum\chi(a)=0$ 知 $S=(-i\pi/f)\Sigma\overline{\chi}(a)a$，即得(1).

现若 χ 为偶特征，同样在 S 中易 a 为 $-a$ 则得

$$\begin{aligned}2S&=\sum_{a}\overline{\chi}(a)(\log(1-\zeta^{-a})+\log(1-\zeta^{a})\\&=2\sum_{a}\overline{\chi}(a)\log|1-\zeta^{a}|=2\sum_{a}\overline{\chi}(a)\log(2\sin\pi a/f)\\&=2\sum_{a}\overline{\chi}(a)\log\sin\pi a/f.\end{aligned}$$

(最后等号是因 $\sum\overline{\chi}(a)=0$). □

设 χ 是模 m 的 Dirichlet 特征，$\zeta=\zeta_m$，$a\in\mathbf{Z}$. 则 χ，ζ^a 的 **Gauss 和**定义为

$$\tau(\chi,\zeta^{a})=\sum_{b=1}^{m-1}\chi(b)\zeta^{ab},$$

其中 a 也可在模 m 的任一剩余系或缩系(或 $\mathbf{Z}/m\mathbf{Z}$ 或$(\mathbf{Z}/m\mathbf{Z})^*$ 的代表元素)中取值求和. 当 χ 为模 m 本原特征而 $\zeta=e^{2\pi i/m}$ 时，

$$\tau(\chi,\zeta)=\tau(\chi)$$

就是上节函数方程中的 Gauss 和. 上述定理证明中对模 $m=f$ 的本原特征 χ 的 Gauss 和 $\tau_a(\chi)$，显然就是 $\tau(\chi,\zeta^a)$.

当 $(c,m)=1$ 时，显然有

$$\begin{aligned}\tau(\chi,\zeta^{ac})&=\sum_{b}\chi(b)\zeta^{abc}=\sum_{b}\chi(c)^{-1}\chi(b\chi)\zeta^{abc}\\&=\overline{\chi}(c)\tau(\chi,\zeta^{a}).\end{aligned}$$

引理 1 若$(a, m) \neq 1$，χ是模m本原特征，则

$$\tau_a(\chi) = \tau(\chi, \zeta^a) = 0.$$

证明 记$d=(a, m)$，$m=rd$. 于是ζ^a是r次本原单位根. 当$k \equiv 1 \pmod r$时，$\zeta^{ak} = \zeta^a$. 因χ本原，故存在整数$k \equiv 1 \pmod r$，$(k, m)=1$，使$\chi(k) \neq 1$. 于是

$$\begin{aligned}\tau_a(\chi) &= \sum_{b=1}^{m-1} \chi(b)\zeta^{ab} = \sum_b \chi(kb)\zeta^{akb} \\ &= \chi(k)\sum_b \chi(b)\zeta^{akb} \\ &= \chi(k)\sum_b \chi(b)\zeta^{ab} = \chi(k)\tau_a(\chi).\end{aligned}$$

即知$\tau_a(\chi) = 0$. □

引理 2 (1) (Gauss 和分解). 设整数$m = m_1 \cdots m_r$且m_i两两互素$(1 \leqslant i \leqslant r)$，$\chi = \chi_1 \cdots \chi_r \in \prod_i \hat{G}_{m_i} = \hat{G}_m$，$\zeta = \zeta_m$，$\zeta_i = \zeta^{m/mi}$. 则

$$\tau(\chi, \zeta^a) = \prod_{i=1}^{r} \chi_i(m/mi)\tau(\chi_i, \zeta_i^a).$$

(2) 设$m = p^s$为素数p的幂，$\chi \in \hat{G}_m$，$\zeta = \zeta_m$. 则$\tau(\chi, \zeta) = 0$当且仅当$s > 1$且χ对模m不本原.

(3) $|\tau(\chi)| = \sqrt{f_\chi}$ （对任意D— 特征χ).

证明 (1) 令$M_i = m/m_i$，则有$t_i \in \mathbf{Z}$使

$$t_1 M_1 + \cdots + t_r M_r = 1$$

于是$s^1 = \prod_i \zeta^{t_i M_i} = \prod \zeta_i^{t_i}$，故

$$\tau(\chi, \zeta^a) = \sum_{b \in G_m} \chi(b) \zeta^{ab}$$
$$= \sum_{b_1 \in G_{m_1}} \cdots \sum_{b_r \in G_{m_r}} \chi(b_1) \cdots \chi(b_r) \zeta_1^{t_1 ab_1} \cdots \zeta_r^{t_r ab_r}.$$

由于 $G_m = G_{m_1} \cdots G_{m_r}$，故

$$\tau(\chi, \zeta^a) = \sum_{b_1} \chi_1(b_1) \zeta_1^{t_1 ab_1} \cdots \sum_{b_r} \chi_r(b_r) \zeta_r^{t_r ab_r}$$
$$= \tau(\chi_1, \zeta_1^{t_1 a}) \cdots \tau(\chi_r, \zeta_r^{t_r a}).$$

注意 $\tau(\chi_i, \zeta_i^{t_i a}) = \overline{\chi}_i(t_i) \tau(\chi_i, \zeta_i^a)$. 又因 $t_i M_i \equiv 1 \pmod{m_i}$，故 $\overline{\chi}_i(t_i) = \chi_i(M_i) = \chi_i(m/m_i)$. 即得(1).

(2) 若 $s = 1$ 且 $\chi = 1$，则 $\tau(\chi, \zeta) = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1 \neq 0$. 故可设 $s \geqslant 1$ 且当 $r = 1$ 时 χ 是本原的(即相当于 $\chi \neq 1$).

$$|\tau(\chi, \zeta)|^2 = \sum_{a \in G_m} \chi(a)^{-1} \zeta^{-a} \sum_{b \in G_m} \chi(b) \zeta^b$$
$$= \sum_{a, b} \chi(a^{-1} b) \zeta^{b-a}$$
$$= \sum_a \sum_{t \in G_m} \chi(t) \zeta^{at-a} \quad (t = a^{-1} b).$$
$$= \sum_t \chi(t) \sum_a \zeta^{a(t-1)}$$
$$= \sum_t \chi(t) \sum_a \zeta^{a(t-1)} - \sum_t \chi(t) \sum_{c \in G_{m'}} \zeta^{pc(t-1)},$$

其中 $m' = p^{s-1}$. 第一项中，若 $t \not\equiv 1 \pmod{p^s}$，则对 a 的求和为 0，故第一项为 p^s. 同样，若 $s > 1$ 而 $t \not\equiv 1 \pmod{p^{s-1}}$，则对 c 求和为 0. 故知

$$|\tau(\chi, \zeta)|^2 = p^s - p^{s-1} \sum_{\substack{t \in G_m \\ t \equiv 1 \pmod{m'}}} \chi(t).$$

当 $s = 1$ 时，此处和式等于 $\sum_{t \in G_p} \chi(t)$，恰为 0. 当 $r > 1$ 且 χ 为本原时，χ 在 G_m 的子群 $\{t \mid t \equiv 1 \pmod{m'}\} = H$ 上的限制非平凡，

故上述和式也为 0. 最后，若 $r>1$ 且 χ 非本原，显然 χ 在子群 H 上平凡，故上述和式等于 p.

(3) 记 $f=p_1^{e_1}\cdots p_r^{e_r}$，$\chi=\chi_1\cdots\chi_r$. 每个 χ_i 的导子为 $p_i^{e_i}$；否则 χ_i 在子群 $\{a\,|\,a\equiv 1(\bmod\ p_i^{e_i-1})\}=H_i$ 上平凡，χ 在 $\{a\,|\,a\equiv 1 \bmod f/p_i\}$ 上平凡，χ 非本原. 由(1)知 $|\tau(\chi)|^2=\prod|\tau(\chi_i)|^2$. (2) 的证明已说明，若 χ_i 模 $p_i^{e_i}$ 本原，则 $|\tau(\chi,\zeta)|^2=p_i^{e_i}$. □

设 K 为二次数域，则 $\hat{K}=\{1,\chi\}$. 由定理 1 知判别式 $D=D(K)=\pm f_\chi=\pm f$. 此时特征 χ 与 Legendre—Kronecker 符号是一致的，即若 p 为奇素数，则有

$$\chi(p)=\left(\frac{D}{p}\right)=\begin{cases}1, & \text{若 } D \text{ 为模 } p \text{ 平方剩余},\\ -1, & \text{若 } D \text{ 为模 } p \text{ 非平方剩余},\\ 0, & \text{若 } p\,|\,D.\end{cases}$$

$$\chi(2)=\left(\frac{D}{2}\right)=\begin{cases}1, & \text{当 } D\equiv 1(\bmod 8),\\ -1, & \text{当 } D\equiv 5(\bmod 8),\\ 0, & \text{当 } D\equiv 0(\bmod 4).\end{cases}$$

事实上，$\left(\frac{D}{p}\right)=1,\ -1,\ 0$ 分别相当于 p 在 K 中分裂，惯性，分歧. 由上章 §8.2 定理 2 知，这分别相当于 $\#Z=2$；$\#Y=2$；$\#Z=1$，$\#Y=1$. 这就相当于 $\chi(p)=1,\ -1,\ 0$. 此外，由 $p\in(\mathbf{Z}/f\mathbf{Z})^*$(的限制)即为 K 的 Frobenius 自同构 σ，也易直接得出上述结论. $\chi(2)$ 与此同理可得.

定理 3 设 K 为二次数域，$\langle\chi\rangle=\hat{K}$，$d=|\mathrm{Disc}(K)|$. 当 K 为实域时设 $\epsilon>1$ 是 K 的基本单位，则 K 的类数

$$h=\frac{-1}{\log\epsilon}\sum_{0<a<d/2}\chi(a)\log\sin\pi a/d \qquad (\text{当 } K \text{ 为实域}).$$

$$h = \frac{-1}{d} \sum_{0<a<d} \chi(a)a$$

$$= (2-\chi(2))^{-1} \sum_{0<a<d/2} \chi(a) \text{（当 } K \text{ 为虚域，} d>4\text{）.}$$

证明　先设 K 为实域，由定理 2 知 $h = h_K$ 为

$$h = \frac{-\sqrt{d}\,\tau(\chi)}{2Rf} \sum_{a=1}^{f} \overline{\chi}(a) \log \sin(\pi a/f).$$

其中 $f = f_\chi = d$（见 §7.4 定理 2）. 定理 1(2) 中已证明 $\tau(\chi) = \sqrt{f}$. 又因 $\chi(f-a) = \chi(-a) = \chi(a)$，$\sin \pi(f-a)/f = \sin \pi a/f$，故对 a 的求和可限于 $0 < a < d/2$. 再因正规子 $R = \log \varepsilon$，即得实二次域的公式.

再设 K 为虚二次域，仍有 $f = f_\chi = d = d_K$（见 §7.4）. $d > 4$ 使得 K 的单位只有 ± 1. 于是由定理 2 知 $h = h_K$为

$$h = (\sqrt{d}\, i\tau(\chi)/d^2) \sum_{0<a<f} \chi(a)a.$$

再由定理 1(2)，当 K 为二次域时 $\hat{K} = \langle 1, \chi \rangle$ 而 $\tau(\chi) = 1$，即知 $\tau(\chi) = i\sqrt{d} = i\sqrt{f}$. 这就得到关于虚二次域的第一个类数公式.

现证虚域的后一公式，先设 f 是偶数. 自然同态 $G_f \to G_{f/2}$ 的核由 $1 + f/2 \pmod f$ 生成，故 $\chi(1+f/2) = -1$. 若 $(y, f) = 1$，则 $1 + yf/2 \equiv 1 + f/2 \pmod f$，故 $\chi(1+yf/2) \equiv -1$. 对任意 a，若 $(a, f) = 1$，则 $a + f/2 \equiv a(1 + a^{-1}f/2) \pmod f$，故 $\chi(a + f/2) = -\chi(a)$.

于是

$$hf = -\sum_{0<a<f/2} \chi(a)a - \sum_{0<a<f/2} \chi(a+f/2)(a+f/2)$$

$$= -\sum_{0<a<f/2} \chi(a)a + \sum_{0<a<f/2} \chi(a)(a+f/2)$$

$$= \frac{f}{2} \sum_{0<a<f/2} \chi(a).$$

注意此时 $\chi(2) = 0$，故 f 偶数情形得证.

最后设 f 为奇数，则有

$$hf = - \sum_{0<a<f/2} \chi(a)a - \sum_{0<a<f/2} \chi(f-a)(f-a)$$

$$= - \sum_{0<a<f/2} \chi(a)a + \sum_{0<a<f/2} \chi(a)(f-a),$$

$$hf = \sum_{0<a<f/2} \chi(a)(f-2a). \qquad (*)$$

另一方面又有

$$hf = - \sum_{0<a<f} (\chi(a)a + \chi(f-a)(f-a)) \text{（其中 } a \text{ 为偶数）}$$

$$= -2 \sum_{0<a<f/2} \chi(2a)a - 2 \sum_{0<a<f/2} \chi(2a)a + f \sum_{0<a<f/2} \chi(2a)$$

$$= -4 \sum_{0<a<f/2} \chi(2a)a + f \sum_{0<a<f/2} \chi(2a).$$

即知

$$hf\chi(2) = \sum_{0<a<f/2} \chi(a)(-4a+f). \qquad (**)$$

将(*)式乘以 -2 加到(**)式则有

$$hf(-2+\chi(2)) = -f \sum_{0<a<f/2} \chi(a).$$

这就证明了定理 3. □

系 1 (1) 设 K 为实二次域，则

$$\varepsilon^h = \Big(\prod_{\chi(b)=-1} \sin \pi b/d\Big) \Big/ \Big(\prod_{\chi(a)=1} \sin \pi a/d\Big),$$

其中整数 a, b 属于区间 $(0, d/2)$ 均与 d 互素，$\langle\chi\rangle = \hat{K}$.

(2) 设 $K = \boldsymbol{Q}(\sqrt{-p})$，素数 $p \equiv 3 \pmod 4$，则类数 h 为奇数. 且

$$h = \begin{cases} R - N, & \text{当 } p \equiv 7 \pmod 8 \\ (R - N)/3, & \text{当 } p \equiv 3 \pmod 8 \end{cases}$$

其中R, N是区间$(0, p/2)$中模p平方剩余和非剩余整数个数.

证明 (1) 在定理 3 上式取指数.

(2) 由定理 3 下式知 $h = (2 - \chi(2))^{-1} \sum_{0<a<p/2} \chi(a)$，和恰为 $R-N$ 且为奇数(共奇数项). 即得引理. 注意由引理可知 $R > N$, 故平方剩余在区间$(0, p)$的前半段较密. □

以下重要结论易由引理 2 中 Gauss 和的性质和域的特征性质得到：设 Abel 数域 $K \subset Q((\zeta_m) = L_m$，$m$ 是 K 的导子，η 为 ζ_m 的 L_m 到 K 的迹，则 $K = Q(\eta)$. 而且当 m 为奇素数时 η 的共轭元集形成 K 的整基(正规整基).

§ 8.6 Bernoulli 数

Bernoulli 数 B_n由下式定义：

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

广义 Bernoulli 数 $B_{n,\chi}$ 由下式定义：

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

其中 $f = f_\chi$ 为特征 χ 的导子. 注意当 $\chi = 1$ 时，上式左方为

$$\frac{te^{at}}{e^t - 1} = \frac{t}{e^t - 1} + t.$$

故 $B_{n,1} = B_n$(当 $n \geqslant 2$)，而 $B_{1,1} = \frac{1}{2}$, $B_1 = -\frac{1}{2}$. 当 $\chi \neq 1$ 时

总有 $B_{-0,\chi}=0$，因为 $\sum_{1}^{f}\chi(a)=0$.

Bernoulli 多项式 $B_n(X)$ 如下定义：

$$\frac{te^{Xt}}{e^t-1}=\sum_{n=0}^{\infty}B_n(X))\frac{t^n}{n!}.$$

简单的计算可知有

$$B_n(1-X)=(-1)^nB_n(X),$$

$$B_n(X)=\sum_{i=0}^{n}C_n^iB_iX^{n-i},$$

后者是因为 $B_n(X)$ 的生成函数是以下两式的积：

$$\frac{t}{e^t-1}=\sum B_n\frac{t^n}{n!},\qquad e^{Xt}=\sum X^n\frac{t^n}{n!}.$$

引理 1 设 $f|F$ 则

$$B_{n,\chi}=F^{n-1}\sum_{a=1}^{F}\chi(a)B_n(a/F).$$

证明 记 $g=F/f$，$a=b+cf$，则由下式即得：

$$\sum_{n=0}^{\infty}F^{n-1}\sum_{a=1}^{F}\chi(a)B_n(a/F)\frac{t^n}{n!}=\sum_{a=1}^{F}\chi(a)\frac{te^{(a/F)Ft}}{e^{Ft}-1},$$

$$\sum_{b=1}^{f}\sum_{c=0}^{g-1}\chi(b)\frac{te^{(b+cf)t}}{e^{fgt}-1}=\sum_{b=1}^{f}\chi(b)\frac{te^{bt}}{e^{ft}-1}=\sum_{n=0}^{\infty}B_{n,\chi}\frac{t^n}{n!}.$$

□

特别，因 $B_1(X)=X-\frac{1}{2}$，故有

$$B_{1,\chi}=f^{-1}\sum_{a=1}^{f}\chi(a)a\qquad(\chi\neq1).$$

$B_{n,\chi}$ 的定义函数是 t 的偶(当 χ 偶) 或奇(当 χ 奇) 函数，故

$$B_{n,\chi} = 0 \quad (\text{当 } n,\ \chi \text{ 不同奇偶})(B_{1,1} \text{ 例外}).$$

定理 1 (1) $L(1-n, \chi) = -B_{n,\chi}/n$，当 n 为正整数.

(2) $\zeta(1-n, b) = -B_n(b)/n$，$0 < b \leqslant 1$，$n \geqslant 1$ 为整数，其中 $\zeta(s, b) = \sum_{n=0}^{\infty}(b+n)^{-s}$ 为Hurwitz Zeta 函数($\mathrm{Re}(s) > 1$).

证明 注意

$$L(\zeta, \chi) = \sum_{a=1}^{f} \chi(a) f^{-s} \zeta(s, a/f).$$

令

$$F(t) = \frac{t\exp((1-b)t)}{\exp(t)-1} = \sum_{n=0}^{\infty} B_n(1-b)t^n/n!$$

在复平面上沿下列途径作积分 $H(s) = \int F(z)z^{s-2}dz$：由 $+\infty$ 沿实轴上方左行至 0 附近；沿以 0 为中心，ε 为半径的圆 C_ε 逆时针行至实轴下方；沿实轴下方右行至 $+\infty$. 令 $z^s = \exp(s\log z)$，其中对数 log 在实轴上方取值 $\log t$，在实轴下方取值 $\log t + 2\pi i$. 显然 $H(s)$ 对所有 s 有定义且解析. 故有

$$H(s) = (e^{2\pi is} - 1)\int_{\varepsilon}^{\infty} F(t)t^{s-2}dt + \int_{C_\varepsilon} F(z)z^{s-2}dz$$

先设 $\mathrm{Re}(s) > 1$，于是 $\int_{C_\varepsilon} \to 0$(当 $\varepsilon \to 0$). 故

$$H(s) = (e^{2\pi is} - 1)\int_0^{\infty} F(t)t^{s-2}dt,$$

$$\begin{aligned}\int_0^{\infty} F(t)t^{s-2}dt &= \int_0^{\infty} t^{s-1}\sum_{m=0}^{\infty} e^{-(b+m)t}dt \\ &= \sum_{m=0}^{\infty}\int_0^{\infty} t^{s-1}e^{-(b+m)t}dt\end{aligned}$$

$$= \sum_{m=0}^{\infty}(m+b)^{-s}\Gamma(s) = \Gamma(s)\zeta(s, b).$$

故 $\zeta(s, b) = H(s)/(e^{2\pi is}-1)\Gamma(s)$，通过解析开拓，这关系对所有 $s \neq 1$ 成立．这也给出 $\zeta(s, b)$ 的解析开拓．

现设 $s = 1 - n$，n 为正整数．则 $e^{2\pi is} = 1$，故

$$H(1-n) = \int_{C_\varepsilon} F(z)z^{-n-1}dz = (2\pi i)B_n(1-b)/n!$$

由于

$$\lim_{s\to 1-n}(e^{2\pi is}-1)\Gamma(s) = (2\pi i)(-1)^{n-1}/(n-1)!,$$

故

$$\zeta(1-n, b) = (-1)^{n-1}B_n(1-b)/n = -B_n(b)/n.$$

$$L(1-n, \chi) = \sum_{a=1}^{f}\chi(a)f^{n-1}\zeta(1-n, a/f)$$

$$= -n^{-1}\sum_{a}\chi(a)f^{n-1}B_n(a/f) = -B_{n,\chi}/n.$$

□

当 χ 为奇特征时，由 §8.4 末的函数方程及此处定理 1 可知 $L(1, \chi)$ 也可表为

$$L(1, \chi) = \tau(\chi)2\pi/(2if)L(0, \bar{\chi})$$

$$= \pi i\tau(\chi)f^{-1}B_{1,\bar{\chi}}.$$

以下讨论 CM- 域，这是虚二次域和分圆域的推广．一个 CM- 域 K 就是全实数域 K^+ 的一个全虚二次扩张．也就是说，CM- 域 K 可如下得到：

$$K = K^+(\sqrt{a}),$$

其中 K^+ 为全实数域，$a \in K^+$ 的所有共轭均为负数．我们回

忆，一个数域 F 称为全实的是指 F 到 $\mathbf{C}$ 的每个嵌入均在 $\mathbf{R}$ 内；F 称为全虚的是指它到 $\mathbf{C}$ 的每个嵌入均不在 $\mathbf{R}$ 内. 例如 $K = \mathbf{Q}(\zeta_m)$ 是 CM- 域，$K^+ = \mathbf{Q}(\zeta + \zeta^{-1})$，记 $a = \zeta^2 + \zeta^{-2} - 2$ 则 $K = K^+(\sqrt{a})$. 这里 a 即为 $X^2 - (\zeta + \zeta^{-1}) + 1$ 的判别式，$\zeta = \zeta_m$. 对 CM- 域 K，我们不妨认为 $K \subset \mathbf{C}$，从而 K 中元素 α 有复共轭 $\bar{\alpha}$.（事实上，易知 K 到 $\mathbf{C}$ 的嵌入的不同不影响 K 的复共轭自同构：若 φ，ψ 是 K 到 $\mathbf{C}$ 的两个不同嵌入，且 $\overline{\varphi(\alpha)} = \varphi(\beta)$，则必有 $\overline{\psi(\alpha)} = \psi(\beta)$，亦即必有 $\varphi^{-1}\bar{\varphi} = \psi^{-1}\bar{\psi}$，其中 $\bar{\varphi}(\alpha) = \overline{\varphi(\alpha)}$. 这是因为 $\bar{\varphi}(K) = K$，从而 $\varphi^{-1}\bar{\varphi}$ 和 $\psi^{-1}\bar{\psi}$ 均为 K/K^+ 的非平凡自同构，必相等).

定理2 设 K 为 n 次 CM- 域，K^+ 为其最大实子域，h 和 h^+ 分别为它们的类数，U 和 U^+ 为其单位群，R 和 R^+ 为其正规子，W 为 K 的单位根群，$w = \#W$，则

(1) $h^- = h/h^+$ 为整数（称为相对类数，或 h 的第 1 因子）.

(2) $Q := [U : WU^+] = 1$ 或 2，

(3) $R/R^+ = 2^{r-1}/Q \qquad (r = n/2)$

(4) $h^- = Qw \prod_{奇\chi \in \hat{K}} \left(-\frac{1}{2}B_{1,\chi}\right)$.

定理 3 设 K/k 是数域扩张，不含非分歧的 Abel 子扩张（指对所有素除子），则 $h_k | h_K$.（对无限素除子，若实除子延拓为虚除子，则称为分歧且分歧指数为 2；否则称为非分歧）. 特别当 K/k 对某素除子 $\wp$ 完全分歧时，或者当 K/k 正规且 Galois 群为非Abel 单群时，$h_k | h_K$.

引理 1 若 α 为代数整数且所有共轭的（复数）绝对值均等

于 1(也就是说 α 的阿基米德赋值均为 1)，则 α 是单位根.

定理3的证明 需用类域论(见下章). 设 H 是 k 的 Hilbert 类域，即最大非分歧(在所有素除子)Abel 扩张，则 $\mathrm{Gal}(K/k)\cong C(k)$($k$ 的理想类群). 由定理所设知 $H\cap K=k$，故 $[HK:K]=[H:k]=h_k$. 因 KH/K 是非分歧 Abel 扩张，必含于 K 的 Hilbert 类域 H_K 中，故 h_k 是 $h_K=[H_K:K]$的因子. □

引理 1 证明 α^j 满足一个多项式 $f(X)\in\mathbf{Z}[X]$，$f(X)$ 的系数是 α^j 的共轭元的初等对称函数，它们的绝对值均为 1. 故 $f(X)$ 的系数 a_i 均满足 $|a_i|\leqslant C_n^i$(其中 $n=\deg f\leqslant[\mathbf{Q}(\alpha):Q]$). 这样的多项式 $f(X)\in\mathbf{Z}[X]$ 只有有限多个，故 $\alpha^j(j\in\mathbf{Z})$ 只有有限个取值，即必有 $t\neq j$ 使 $\alpha^t=\alpha^j$，从而 $\alpha^{t-j}=1$，即知 α 是单位根. □

定理 2 的证明 (1) 由于 K/K^+ 对无限素除子完全分歧，故满足定理 3，即知 $h^+|h$.

(2) 因 K 为 CM—域，故 $\varepsilon/\bar{\varepsilon}$ 的所有共轭的绝对值均为 1(其中 ε 为 K 的单位)，故由引理 1 知 $\varepsilon/\bar{\varepsilon}$ 为单位根. 故由 $\varepsilon\longmapsto\varepsilon/\bar{\varepsilon}$ 可定义 $\varphi:U\to W$，并诱导出 $\psi:U\to W/W^2$. 设 $\varepsilon=\zeta\varepsilon_1$，其中 $\varepsilon_1\in U^+$，$\zeta\in W$，则 $\varepsilon/\bar{\varepsilon}=\zeta^2\in W^2$，$\varepsilon\in\mathrm{Ker}\psi$. 反之，若 $\varepsilon/\bar{\varepsilon}=\zeta^2\in W^2$，则易知 $\varepsilon_1=\varepsilon/\zeta\in U^+$. 故 $\mathrm{Ker}\psi=WU^+$. 因 $(W:W^2)=2$，定理得证. 同时可注意，若 $\varphi(U)=W$ 则 $Q=2$；若 $\varphi(U)=W^2$ 则 $Q=1$.

(3) **正规子** R_K 的定义可简述如下(见 §6.4 及其习题). 设 $\eta_1,\cdots,\eta_{r-1}$ 是 K 的基本单位系，σ_i 是 K 到 $\mathbf{C}$ 的嵌入，则 R_K 为

下述行列式的绝对值：

$$\det(n_i \log|\sigma_i \eta_j|) \qquad (1 \leqslant i,\ j \leqslant r-1).$$

这里 $n_i = 1$ 或 2（依 σ_i 为实或虚嵌入）. R_K 可解释为 U 到 $\mathbf{R}^{r-1}$ 嵌入象所成格的基本区的体积测度. 稍作推广，K 的任一组（相互独立）的单位 $\varepsilon_1, \cdots, \varepsilon_{r-1}$ 的（相对于 K）的正规子定义为

$$R_K(\varepsilon_1, \cdots, \varepsilon_{r-1}) = |\det(n_i \log|\sigma_i \varepsilon_j|)| \qquad (1 \leqslant i,\ j \leqslant r-1).$$

当然若 $\varepsilon_1, \cdots, \varepsilon_{r-1}$ 不是相互独立的，则其**正规子**为 0（由上述几何意义）. $r = r_1 + r_2$ 如第六章.

引理 2 设 $\{\varepsilon_i\}$ 和 $\{\eta_i\}$ 为数域 K 的两组独立单位，各生成单位子群 A 和 B，若 $A \subset B$ 且指数有限，则

$$(B : A) = R_K(\varepsilon_1, \cdots, \varepsilon_{r-1}) / R_K(\eta_1, \cdots, \eta_{r-1}).$$

证明 可设

$$\varepsilon_i = \zeta_i \prod_j \eta_j^{a_{ij}} \qquad (a_{ij} \in \mathbf{Z},\ \zeta_i \in W),$$

则

$$n_i \log|\sigma_S \varepsilon_i| = \sum_j a_{ij} n_i \log|\sigma_S \eta_j|.$$

故

$$R_K(\varepsilon_1, \cdots, \varepsilon_{r-1}) / R_K(\eta_1, \cdots, \eta_{r-1}) = |\det(a_{ij})|.$$

由线性代数（或主理想环上模）理论可知，对整系数方阵 (a_{ij})，存在行列式为 ± 1 的整系数方阵 M, N 使 $M(a_{ij})N = \mathrm{diag}(d_1, \cdots, d_{r-1}) = D$（如见[Zh22]）. 于是 $\det(a_{ij}) = \pm \prod d_i$. 而 $M = (m_{ij})$, $N = (n_{ij})$ 分别相当于 A 和 B 的基变换： $\varepsilon_i' = \prod \varepsilon_j^{m_{ij}}$, $\eta_i' = \prod \eta_j'^{n_{ij}}$，于是 $\varepsilon_i' = \prod_j \eta_j'^{d_{ij}} = \eta_i'^{d_i}$, $(d_{ij}) = (D)$. 故 $(B : A) = |d_1 \cdots d_{r-1}| = |\det(a_{ij})|$. 引理得证. □

现回到定理 2(3) 的证明. 由(2) 知, K^- 的基本单位系 ε_1, $\cdots$, ε_{r-1} 在 U 中生成指数为 Q 的子群 WU^-. 但对 K^+ 而言 $n_i=1$, 而对 K 而言 $n_i=2(1\leqslant i<r)$. 故有

$$R=R_K(\varepsilon_1,\cdots,\varepsilon_{r-1})Q=R_{K^+}(\varepsilon_1,\cdots,\varepsilon_{r-1})2^{r-1}Q$$
$$=R^+2^{r-1}Q$$

(4) 设 $X=\hat{K}$ 为 K 的特征群. 因 K 全虚, 故奇、偶特征数均为 $n/2=[K:\mathbf{Q}]/2$. 由 §8.5 引理 1 有

$$R^+h^+=\frac{2\sqrt{d(K^+)}}{2^{n/2}}\prod_{1\neq\chi\text{偶}}L(1,\chi),$$

$$Rh=\frac{w\sqrt{d(K)}}{(2\pi)^{n/2}}\prod_{1\neq\chi\in\hat{K}}L(1,\chi),$$

二式相除则得

$$hR/(h^+R^+)=\frac{w\sqrt{d(K)}}{2\pi^{n/2}\sqrt{d(K^+)}}=\prod_{\chi\text{奇}}L(1,\chi).$$

而由定理 1 的推论知, 对奇特征 χ 有 $L(1,\chi)=\pi i\tau(\chi)f_\chi^{-1}B_{1,\bar{\chi}}$. 由导子一判别式定理(§8.5 定理 1) 知 $\sqrt{d(K)/d(K^+)}=(\prod_{\chi\text{奇}}f_\chi)^{1/2}$. 由 §8.5 定理 1(2) 知 $\prod_{\chi\text{奇}}\tau(\chi)=i^{n/2}\sqrt{d(K)/d(K^+)}$. 即得定理 2. □

定理 4 设 $K=Q(\zeta_m)$, $K^+=Q(\zeta_m+\zeta_m^{-1})$. 则

(1) $Q=1$ 或 2 (各依 m 为素数幂或否).

(2) $C^+\to C$ 为自然嵌入, 其中 C 和 C^+ 为 K 和 K^+ 的理想类群.

证明 (1) 当 m 为奇素数幂时, §7.6 定理 2 已证. 设 $m=$

2^S，$\varepsilon \in U$，$\varepsilon/\bar{\varepsilon} \notin W^2$（见定理 2 证明），则 $\varepsilon/\bar{\varepsilon} = \zeta$ 是 m 次本原单位根. 以 N 表示由 K 到 $\boldsymbol{Q}(\sqrt{-1}) = \boldsymbol{Q}(i)$ 的范映射. 则 $N(\zeta) = \zeta^a$，其中

$$a = \sum_{\substack{0<b<m \\ b\equiv 1(4)}} b = \sum_{j=0}^{m/4-1}(1+4j) = 2^{S-2} + 2^{S-1}(2^{S-2}+1)$$
$$\equiv 2^{S-2}(\mathrm{mod}\, 2^{S-1}).$$

故 $\zeta^a = \pm i$ 是本原 4 次单位根，从而 $N(\varepsilon)/\overline{N(\varepsilon)} = \pm i$. 因 $N(\varepsilon)$ 是 $\mathbf{Q}(i)$ 的单位，故 $N(\varepsilon) = \pm 1$，$\pm i$，均矛盾. 故总有 $\varepsilon/\bar{\varepsilon} \in W^2$，$Q = 1$.

再设 m 不是素数幂，由 §7.6定理1知 $1-\zeta_m = \varepsilon$ 是单位，设 $\varepsilon/\bar{\varepsilon} = -\zeta_m \in W^2$，则 $-\zeta_m = -\zeta = (\pm\zeta^r)^2 = \zeta^{2r}$，$-1 = \zeta^{2r-1}$. 显然 m 须为偶数，从而 $m \equiv 0(\mathrm{mod}\ 4)$. 由 $-1 = \zeta^{n/2}$ 有 $n/2 \equiv 2r-1(\mathrm{mod}\ m)$，故 $n/2 \equiv -1(\mathrm{mod}\ 2)$，此不可能. 故 $-\zeta \notin W^2$，$Q = 2$.

(2) 首先，K^+ 的每个理想 I 在 K 中生成一个理想 $I' = IO_K$. 主理想仍生成主理想，故有自然映射 $C^+ \longrightarrow C$. 现若 I' 为主理想，我们需要证明 I 也为主理想. 设 $I' = (\alpha)$，$\alpha \in K$. 则 $(\bar{\alpha}/\alpha) = \bar{I}'/I' = \bar{I}O_K/IO_K = (1)$，故 $\bar{\alpha}/\alpha$ 为单位，处处绝对值为 1，故由引理 1 知 $\bar{\alpha}/\alpha$ 为单位根. 若 m 不是素数幂，则 $Q = 2$，定理 2(2) 的证明显示有单位 ε 使 $\varepsilon/\bar{\varepsilon} = \bar{\alpha}/\alpha$，则 $\alpha\varepsilon \in K^+$ 且 $I' = (\alpha) = (\alpha\varepsilon)$. 故 $I = (\alpha\varepsilon) = \alpha\varepsilon O_{K^+}$，即知 I 是主理想. 再设 $m = p^S$ 为素数幂，令 $\pi = \zeta_m - 1 = \zeta - 1$，则 $\pi/\bar{\pi} = -\zeta$ 生成 K 的单位根群 W. 故 $\bar{\alpha}/\alpha = (\pi/\bar{\pi})^d$（$d$ 为某整数）. $\wp = (\pi)$ 在 K 中完全分歧，故 $\wp$-adic 指数赋值在 K^+ 中只取偶数值. 又因 $\alpha\pi^d$ 和 I 均属于 K^+，故

$d = v_\wp(\alpha\pi^d) - v_\wp(\alpha) = v_\wp(\alpha\pi^d) - v_\wp(I)$ 为偶数. 故 $\bar{\alpha}/\alpha =$

$(-\zeta)^d \in W^2$. 特别 $\bar{\alpha}/\alpha = \zeta_1/\bar{\zeta_1}$, $\alpha\zeta_1 \in K^+$, ζ_1 是某单位根. 即知 $I = (\alpha\zeta)$ 为主理想. □

§ 8.7 进一步的解析理论

先稍介绍一些 p-adic L-函数知识及应用. 设 p 为素数, $\boldsymbol{Q}_p$ 为 p-adic (有理) 数域, 设 $\bar{\boldsymbol{Q}}_p$ 为其代数闭包. p-adic 赋值记为 $|p| = |p|_p = 1/p$, 到 $\bar{\boldsymbol{Q}}_p$ 有唯一延拓.

可以证明, $\bar{\boldsymbol{Q}}_p$ 不是完备的($\sum\limits_n \zeta_{n'} p^n \notin \bar{\boldsymbol{Q}}_p$, 其中 $n' = n$ 或 1(依 $(n, p) = 1$ 或否)). 所以我们将 $\bar{\boldsymbol{Q}}_p$ 完备化为 $\boldsymbol{C}_p$. 容易证明 $\boldsymbol{C}_p$ 是代数封闭的. (注意, 序列 $\boldsymbol{Q}_p \longrightarrow \bar{\boldsymbol{Q}}_p \longrightarrow \boldsymbol{C}_p$ 可与下述序列平行类比(在做 p-adic 分析问题时): $\boldsymbol{Q} \longrightarrow \bar{\boldsymbol{Q}} \longrightarrow \boldsymbol{C}$, 其中 $\bar{\boldsymbol{Q}}$ 表 $\boldsymbol{Q}$ 的代数闭包). 以下在 $\boldsymbol{C}_p$ 中考虑问题. 变元 $X \in \boldsymbol{C}_p$ 的 p-adic 对数和指数函数(即与变元 $X \in \boldsymbol{C}$ 的对数和指数函数有某些类似性质的函数), 可通过级数定义:

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!} \qquad (\boldsymbol{C}_p \text{ 上函数}),$$

$$\log_p(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} X^n}{n} \qquad (\boldsymbol{C}_p \text{ 上函数}).$$

可证明 $\exp(X)$ 的收敛半径为 $|X| < p^{-1/(p-1)} < 1$(注意 $1/n!$ 的 p-adic 值可很大, 故收敛半径很小). 而 $\log_p(1+X)$ 的收敛半径为 $|X| < 1$. 不过 $\log_p$ 可唯一开拓到 $\boldsymbol{C}_p^*$ 上, 满足 $\log_p(p) = 0$, $\log_p(ab) = \log a + \log b$. 且 $\log_p a = 0 \Leftrightarrow a = p^b\zeta$($b \in \boldsymbol{Q}$, ζ 是单位根(任意次). a 在 exp 的收敛半径内时, 有 $\log_p \exp(a) = a$, $\exp \log_p(1+a) = 1 + a$.

易知有分解

$$C_p^* = p^Q \times W \times U_1$$

其中W是C_p^*中阶与p互素的单位根全体，$U_1 = \{u \in C_p \mid |u - 1| < 1\}$. 记

$$q = p \text{ 或 } 4 \text{ (当 } p \neq 2 \text{ 或 } p = 2\text{)}.$$

对任意$a \in Z_p$，$p \nmid a$，存在唯一的$\varphi(q)$次单位根$\omega(a) \in Z_p$使

$$a \equiv \omega(a) \qquad (\mathrm{mod}\ q).$$

ω称为 Teichmüller 特征($\omega(a)$显然即a在上述分解中的W-分量). 记$\langle a \rangle = \omega(a)^{-1}a$，则$\langle a \rangle \equiv 1 (\mathrm{mod} q)$.

复变量的L-函数在数域类数等方面十分重要. 能否构造出变量$s \in C_p$的有类似性质的函数呢?这就是构作p-adic L-函数问题. 较好的方法是构作出一个p-adic 函数，它在$1-n$处与$L(s, \chi)$有(基本上)同样的取值. 固定$\overline{Q}$到C_p的一个嵌入. 于是 Dirichlet 特征χ的取值属于$\overline{Q} \subset C_p$. 于是 Teichmüller 特征ω也可视为 Dirichlet 特征，导子为q，阶为$\varphi(q) = p - 1$或 2.

定理 1 设χ为一 Dirichlet 特征，导子为f，F是f和q的倍数. 则存在唯一的p-adic 半纯(若$\chi \neq 1$则全纯)函数$L_p(s, \chi)$，定义于$\{s \in C_p : |s| < qp^{-1/(p-1)}\}$，在 0 和负整数取值为

$$L_p(1-n, \chi) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \ n \geqslant 1.$$

当$\chi = 1$时$L_p(s, 1)$除$s = 1$外解析且在$s = 1$为单极点，留数为$1 - 1/p$. 一般地，有公式

$$L_p(s, \chi) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1 \\ p \nmid a}}^{F}\chi(a)\langle a \rangle^{1-s}\sum_{j=0}^{\infty}C_{1-s}^j(B_j)(F/a)^j.$$

与上章定理 1(1) 中的复变量 L- 函数相比，p-adic L- 函数中多出因子$(1-\chi\omega^{-n}(p)p^{n-1})$，这是$L(s,\chi\omega^{-n})$在 p 的 Euler 乘积因子(之逆). 一般规律都是这样的：复函数过渡到 p-adic 类似函数时，都要去掉 p- 分量(因为若允许 $p|n$，则 $\Sigma 1/n^s$ 对 p-adic 赋值有任意大的项). 注意特征的积 $\chi\omega^{-n}$ 定义为 § 8.1 末意义下. 当 χ 为奇特征时，n 与 $\chi\omega^{-n}$ 奇偶性不同，故 $B_{n,\chi\omega^{-n}}=0$. 故 χ 奇时 $L_p(s,\chi)=0$. χ 偶时 $L_p(s,\chi)$ 不是零函数.

p-adic 函数的好处之一是易求得同余式. 有以下性质(见 [Wa])：

定理 2 (1) 设 $\chi\neq 1$，$pq\nmid f_\chi$，则

$$L_p(s,\chi)=a_0+a_1(s-1)+a_2(s-1)^2+\cdots$$

其中 $|a_0|\leqslant 1$，$p^2|a_i$ $(i\geqslant 1)$.

(2) 设如上，$m,n\in\mathbf{Z}$. 则有 p-adic 整数的同余式：

$$L_p(m,\chi)\equiv L_p(n,\chi)\qquad(\text{mod } p).$$

(3) 设 $m\equiv n\not\equiv 0(\text{mod } p\text{-}1)$ 为偶数正整数.

则

$$\frac{B_m}{m}\equiv\frac{B_n}{n}\qquad(\text{mod } p).$$

更进一步，若 m,n 为偶数正整数且 $m\equiv n$ (mod $(p-1)p^a$)，而 $n\not\equiv 0(\text{mod } p-1)$，则

$$(1-p^{m-1})\frac{B_m}{m}\equiv(1-p^{n-1})\frac{B_n}{n}\qquad(\text{mod } p^{a+1}).$$

(4) 设奇数 $n\not\equiv -1(\text{mod } p-1)$，则有 p-adic 整数同余式：

$$B_{1,\omega^n}\equiv\frac{B_{n+1}}{n+1}\qquad(\text{mod } p).$$

也可由 $L_p(1, \chi)$ 的值，得到类数公式：

定理 3 (1) 设 $\chi \neq 1$ 为 Dirichlet 特征，导子为 f. 记 $\bar{\chi} = \chi^{-1}$, $\zeta = \zeta_f$, $\tau(\chi) = \sum_{a=1}^{f} \chi(a)\zeta^a$. 则

$$L_p(1, \chi) = -\left(1 - \frac{\chi(p)}{p}\right)\frac{\tau(\chi)}{f}\sum_{a=1}^{f}\bar{\chi}(a)\log_p(1 - \zeta^a).$$

(2) 设 K 为 n 次全实 Abel 数域，则

$$\frac{2^{n-1}h(K)R_p(K)}{\sqrt{D(K)}} = \prod_{\substack{\chi \in \hat{K} \\ \chi \neq 1}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1, \chi),$$

其中 $R_p(K)$ 为 p-adic 正规子，完全与复数正规子同样定义为 $\det(n_i \log_p(\sigma_i \eta_j))(1 \leqslant i, j \leqslant r-1)$，其中嵌入 σ_i 的实、虚性以 $\boldsymbol{C}_p$ 到 $\boldsymbol{C}$ 的嵌入计. 正规子 $R_p(K)$ 和判别式 $D(K)$ 定义中的行列式符号(即行的顺序) 可这样选取：取定顺序使对无限赋值有 $R(K)/D(K) > 0$，然后在 p-adic 情形下用同一顺序. 可证明有 $|nR_p(K)/\sqrt{D(K)}|_p \leqslant 1$.

猜想 $R_p(K) \neq 0$ 对任意数域 K 成立(Leopoldt). 这对 Abel 域 K 已得到证明，并可由此推出 $L_p(1, \chi) \neq 0$(当 $\chi \neq 1$ 为偶特征).

p-adic L- 函数有许多应用. 如证明如下定理.

定理 4 设 p 为奇素数，$K = \boldsymbol{Q}(\zeta_p)$，$K^+$ 是 K 的最大实子域，h, h^+ 为其类数，$h^- = h/h^+$. 则

(1) $p | h^- \Leftrightarrow p | B_j \quad (j = 2, 4, \cdots, p-3)$.

(2) $p | h^+ \Rightarrow p | h^-$. 故 $p | h \Leftrightarrow p | B_j \quad (j = 2, 4, \cdots, p-3)$. 其中 B_j 为 Bernoulli 数.

利用 p-adic L- 函数易证明著明的 Ankeny — Artin — Chowla 公式：设$\boldsymbol{Q}(\sqrt{p})$的基本单位为$\varepsilon=(t+u\sqrt{p})/2>1$，$p\equiv 1(\bmod 4)$，则其类数 h 满足：

$$hu/t\equiv B_{(p-1)/2}\qquad(\bmod p).$$

因为$h<\sqrt{p}$，故此式唯一决定h(如果$u\not\equiv 0(\bmod p)$.

在[Zh5, 11, 12]中，对二、三、四次域分别得出一系列 Ankeny — Artin — Chowla 型的公式，许多公式也可以唯一决定类数.

如对实四次循环域K，有唯一的二次子域k，有相对基本单位E(使$N_{K/k}(E)=\mp 1$且与其共轭，k的基本单位及-1生成指数为$Q=1$或2的单位子群). 设$T_{rK/k}(E)=(a+b\sqrt{D(k)})/2$, a, $b\in\boldsymbol{Z}$, $p=r^2+s^2\equiv 1(\bmod 4)$，$s$为偶数，$h^-=h(K)/h(k)$. 则有

(1) 若$K=\boldsymbol{Q}(\sqrt{p+s\sqrt{p}})$, $p\equiv 1(\bmod 8)$，则

$$h\quad(3(a^2+16)/p-b^2)/(2a^2)$$
$$\equiv B_{(p-1)/4}B_{3(p-1)/4}(\bmod p).$$

(2) 若$K=\boldsymbol{Q}(\sqrt{p+s\sqrt{p}})$, $p\equiv 5(\bmod 8)$则

$$h^-\cdot 16C_p\equiv -E_{(p-5)/8}E_{(3p-7)/8}\quad(\bmod p).$$

(3) 若$K=\boldsymbol{Q}(\sqrt{3(p+s\sqrt{p})})$, $5\neq p\equiv 5(\bmod 8)$，则

$$h^-\cdot C_p\equiv A_{(p-1)/4}A_{3(p-1)/4}\quad(\bmod p).$$

其中B_n为 Bernoulli 数，E_n(Euler 数) 和 A_n 定义为

$$\sec t=\sum_n E_n t^{2n}/(2n)!,\ -t/(1+2\mathrm{ch}t)=\sum_n A_n t^n/n!$$

而$C_p=((a^2\pm 16)/p-b^2/3)/(Qa^2)$.

再设 K 为三次循环域，则 K 有一单位

$$\eta = (a + b\tau(\chi) + \bar{b}\,\overline{\tau(\chi)})/3,$$

与其共轭及 -1 生成全单位群(其中 $a \in \mathbf{Z}$, $b \in \mathbf{Q}(\sqrt{-3})$, $\chi \neq 1$ 为 K 的特征)，记 f 为 K 的导子，$e = (p-1)/3$. 则有

(4) 若 $f = p$ 为素数，则

$$h(K)C \equiv \frac{3}{4}B_e B_{2e} \qquad (\text{mod } p);$$

一般地，若 $p|f$, $p \neq 3$, 则

$$h(K)C \equiv \frac{3}{4}B_{e,\chi_e}B_{2e,\chi_e^2} \quad (\text{mod } p),$$

其中 $C = (a^3 - 27)/(fa^3) - b\bar{b}/a^2$, $\chi_e = \chi\omega^{-e}$, B_e 和 $B_{e,\chi}$ 为(广义) Bernoulli 数.

解析理论在数论中有独特的作用，有不断的发展，以下介绍一些著名结果.

Brauer — Siegel 定理 设 K 过在 $\mathbf{Q}$ 上正规的数域的一个序列，满足 $n/\log d \longrightarrow 0$, 则

$$\log(Rh) \sim \log\sqrt{d},$$

其中 n, d, R, h 表示 K 的次数，判别式绝对值，正规子，类数. 若去掉正规条件而假设对某 $\delta > 0$ 在区间 $[1-\delta, 1]$ 中 $\zeta_K(s)$ 无零点，则定理仍成立.

系 1 设 K 过次数固定为 n 的数域序列，则当 $d \to \infty$ 时有 $\log(Rh) \sim \log\sqrt{d}$.

与此相关的结果有：(1) 存在常数 C, 使当数域 $K \neq \mathbf{Q}$ 时，有 $\log(Rh)/\log(d^{1/2}) < C$. (2) 存在常数 C_S 使对所有正规数域 $K/\mathbf{Q}$ 有 $|\log(Rh)| \geq C_S \log d^{1/2}$.

域 K 的素理想子集 M 的 Dirichlet 密度定义为如下极限(如果存在)：

$$\lim_{s\to1^+}\Big(\sum_{\wp\in M}\frac{1}{N\wp^s}\Big)/\log\frac{1}{s-1}.$$

似乎以下的极限称为 M 的密度(通常密度)更合理些：

$$\lim_{n\to\infty}\frac{\#\{\wp\in M: N\wp\leqslant n\}}{\#\{\wp: N\wp\leqslant n\}}.$$

但易证明，若普通密度存在则 Dirichlet 密度也存在且二者相等.

在 §8.4 定理 2(3) 的证明中已得到，当 $s\to1$ 时有

$$\log\zeta_K(s)\sim\sum_{\wp}N\wp^{-s}\sim\sum_{f(\wp)=1}N\wp^{-s}.$$

这里像通常一样，$f(s)\sim g(s)$ 意义为 $f(s)$ 与 $g(s)$ 相差一个在 $S=1$ 解析的函数，因 $\zeta_K(s)$ 在 $s=1$ 为单极点，故

$$\log\zeta_K(s)\sim\log\frac{1}{s-1}.$$

这就说明 K 的以下两素理想集均有 Dirichlet 密度 1： {K 的素理想 $\wp$ 全体}，{剩余次数 $f(\wp)=1$ 的 K 的素理想全体}. 由于分歧的素理想只有限个，可知{完全分裂的 K 的素理想 $\wp$ 全体}的密度也是 1. 因此我们可以说，K 的"几乎"所有素理想 $\wp$ 在 $p=\wp\cap\boldsymbol{Q}$ 上都是完全分裂的. 若 K 是 $\boldsymbol{Q}$ 的 n 次扩张，则每个 $p\in\boldsymbol{Q}$ 在 K 中有 n 个因子 $\wp$，故上述也可转述为："在 K 中完全分裂的 $\boldsymbol{Q}$ 的素理想 (p) 全体"的密度为 $1/n$.

设 K/k 为 Galois 扩张，$S_{K/k}$ 为在扩域 K 中完全分裂的 k 的素理想集. 若 $L\supset K$ 也是 k 的 Galois 扩张，则显然 $S_{L/k}\subset S_{K/k}$.

以符号 $S_1 \prec S_2$ 表示：在相差密度为0理想集的意义下 $S_1 \subset S_2$. 如果 $S_{K/k} \prec S_{L/k}$ 则可断言 $L = K$. 这是由于 $S_{K/k}$ 的密度为 $1/[K:k]$（如同上述 $S_{K/\mathbf{Q}} = 1/n$），故由 $S_{K/k} \prec S_{L/k}$ 则可知 $[K:k] \geqslant [L:k]$. 由此易证如下：

定理 5 设 K/k 为 Galois 扩张，E/k 为有限扩张. 则

$$S_{K/k} \prec S_{E/k} \Leftrightarrow K \supset E.$$

证明 （$\Rightarrow$）设 L/k 是含 E 的最小 Galois 扩张. k 的素理想 $\wp$ 在 E 完全分裂当且仅当它在 L 如此，因为这相当于 E 的每个 k-共轭含于完备化 $k_\wp$.（若 $\wp \in S_{E/k}$，则 $\wp$ 在 E 分裂，$\sigma\wp = \wp$ 在 σE 分裂（对所有 E 的 k－嵌入），故 $\wp$ 在 $\{\sigma E\}$ 生成的域 L 中分裂）. 故 $S_{K/k} \prec S_{E/k} = S_{L/k}$. 于是 KL/k 是 Galois 扩张，$S_{KL/k} = S_{L/k} \cap S_{K/k} \prec S_{K/k}$. 故 $[KL:k] = S_{KL/k}$ 的密度 $\geqslant S_{K/k}$ 的密度 $= [K:k]$. 即知 $KL = K$，$E \subset L \subset K$. □

密度问题与类域论关系密切. 我们先引用下章类域论的某些结论讨论一个重要的密度问题. 设 K/k 为 n 次 Galois 扩张（注意不一定是 Abel 扩张），$G = G(K/k)$. 对给定 $\sigma \in G$，令

$$T_\sigma = \{\wp \mid \wp \text{ 在 } K \text{ 非分歧且} (\mathscr{P}, K/k) = \sigma\}$$

其中 $\wp$ 过 k 的素理想，$\mathscr{P}$ 是 $\wp$ 在 K 的任一素理想因子，$(\mathscr{P}, K/k)$ 是 $\mathscr{P}$ 决定的 Frobenius 映射. 当然每个 $\wp$ 对应的不仅是 σ，而实为 σ 的共轭类：若 $\mathscr{P} \mid \wp$ 则 $\tau\mathscr{P} \mid \wp$，于是 $(\tau\wp, K/k) = \tau\sigma\tau^{-1}$.

定理 6（Tchebotarev 密度定理） 设 K/k 为 n 次 Galois 扩张，则 T_σ 的密度为

$$\delta(T_\sigma) = c/n,$$

其中 c 是 σ 在 $G(K/k)$ 中的共轭元个数.

证明 设 σ 的阶为 f，固定子域为 K^d，则 K/k^d 为 f 次循环域，故是类域，即有 K^d 的模(除子)$\mathfrak{m}$ 对 K/K^d 可许，使 $\mathscr{A}$：$G(K/K^d)=\langle\sigma\rangle\longrightarrow \boldsymbol{I}(\mathfrak{m})/H$，$\wp'\longrightarrow(\wp',K/K^d)$为同构，$\boldsymbol{I}(\mathfrak{m})$为 K^d 的与 $\mathfrak{m}$ 互素的理想群，H 是 $\boldsymbol{I}(\mathfrak{m})$的子群．不妨设 $T_\sigma\subset\boldsymbol{I}(\mathfrak{m})$(否则取 T_σ 中与 $\mathfrak{m}$ 互素的理想仍记为 T_σ，密度不变)．设 $T_{K,\sigma}=\{\mathscr{P}\mid\wp:(\mathscr{P},K/k)=\sigma\}$(其中 $\wp\in T_\sigma$)，记 $\mathscr{P}\cap K^d=\mathscr{P}'$．记 $T_d=\{\mathscr{P}':\mathscr{P}'\mid\wp,\mathscr{P}'\bmod H$ 固定在某类$\}$($\wp$过在 K^d 完全分裂的 k 素理想．$\mathscr{P}'(\bmod H)=\mathscr{A}(\sigma)$)，则显然 $T_{K,\sigma}$与 T_d 间 $1:1$ 对应($\mathscr{P}'$只有一个素因子 $\mathscr{P}$)，因 K/K^d 为循环扩张，我们知道 T_d 的密度(只依赖于在 $\boldsymbol{Q}$ 上剩余类数为 1 的素理想)是 $\delta(T_d)=\dfrac{1}{f}$．另一方面，对固定的 $\wp$，满足$(\mathscr{P},K/k)=\sigma$ 的 $\mathscr{P}\mid\wp$ 的个数为 $\#G_\sigma/\#G_{\mathscr{P}}$($G_\sigma$ 为 G 中与 σ 可换的元素集，$G_{\mathscr{P}}$ 为 $\mathscr{P}$ 的分解(固定)群)．因$(G:G_\sigma)=c$，故 $\#G_\sigma/\#G_{\mathscr{P}}=n/cf$．故 $\delta(T_\sigma)=(1/f)/(n/cf)=c/n$. □

第九章　伊代尔与类域论

类域论是数学诸理论中，体系最完美的一种. 从类域论的一般性结果，可以系统地导出所有的关于二次域，分圆域，库木尔扩域等阿贝尔域，高次互反律等等数论已知结果. 简言之，类域论阐明了域的(理想或伊代尔)类群与该域的 Abel 扩张的关系. 特别，类群与扩张的 Galois 群是同构的. 由此可知类群的定义要推广，否则即如 Q 的类群也是平凡的，就不会有 Q 上的类域论了.

1898～1899 年，Hilbert 在编写 Zahlbericht 之后，对数域结构有了新的解悟，猜想对任一数域 k，存在 Abel 扩张 K/k 使得：

(1) $\mathrm{Gal}(K/k)\cong C(k)$($k$ 的理想类群)；(2) K/k 非分歧(对任意素除子)；(3) $f(\mathfrak{P}\mid\wp)$是使 $\wp^f$ 为主理想的最小正整数 f($\wp,\mathfrak{P}$ 为 k,K 的素理想)；(4) k 的理想到 K 后均为主理想. 此 K 即称为 k 的(Hilbert)类域. Hilbert 对类数 $h(k)=2$ 证明了 K 的存在性. 他的学生 Furtwängler 到 1907 年证明了前 3 条，1930 年证明了(4). 1908 年，H. Weber 引入广义理想类群 $C_m(k)$，对 $C_m(k)$作了类似于 Hilbert 的猜想，证明了类域的唯一性.

1920 年，T. Takagi(高木贞治)对广义理想类群证明了类域的存在性，一定程度上确立了类域论. 但类群与 Galois 群的同

构是靠计算群的阶得到的，对应还不清楚.

1927年，E. Artin证明了类群与Galois群之间的同构由Frobenius(映射)给出(即Artin映射)，从而完成了类域论.

在类域论的表述方面，1936年Chevalley引入伊代尔(idele)，可表述无限扩张，并将证明算术化. 每个广义理想类群均为idele类群的同态象. 从此idele显得越来越重要. 在20世纪40年代后期，Artin在讨论班上用idele讲述类域论，影响很大. 此外，Hasse在1930年代用单代数理论表述类域论，基本定理为：k上的单代数在k上分裂当且仅当它处处局部分裂. 1950年，G. Hochsehild指出仅用上同调语言即可表述类域论，只需2-上闭链而不需单代数. 约同时，A. Weil发现伊代尔类的基本2-上链，也强调上同调方法. 在此基础上，Artin－Tate的著名讲义〔A-T〕在有限群上同调理论基础上，重新构成了类域论. Iyanaga〔Iy〕对此详有论述. 此外，Zorn(1933)由可除代数的Zeta函数的函数方程出发，可得到单代数基本定理，从而得到类域论的另一证明路线，Weil的书〔We〕即采用此路线. J. Neukirch用纯拓扑群论的方法也给出简洁的阐述.

当然，最吸引人的方法当数直接构作出类域从而明显给出互反律(对应)，即所谓Kronecker“青春之梦”(Jugendtraum). 但目前仅对虚二次域(及其推广CM－域)成功，主要是用椭圆曲线理论.

以下将主要用idele语言阐述类域论，利于读者阅读现代文献. 同时也兼顾理想语言，因为由此很易看到Artin映射的自然性，完全舍弃是不适宜的. 整个理论的阐述是经证明的，且基本自足. 将少量使用上同调论(即循环群的“六边形”)，并以多种方式表述类域论的结果，便于读者使用.

设K/k为n次Abel扩张，$\wp$为k的素理想，在K非分歧，

$\mathfrak{P}|\wp$是 K 的素理想，$\overline{K}/\overline{k}$ 是 $f=f(\mathfrak{P}|\wp)$次扩张(这里 $\overline{K},\overline{k}$ 是模 $\mathfrak{P},\wp$剩余类域)．$\overline{k}$ 是 $q=N\wp=p^{f_0}$元有限域($f_0=f(\wp|p)$，$p=\wp\cap\mathbf{Z}$)，故 $\overline{k}=\boldsymbol{F}_q,\overline{K}=\boldsymbol{F}_{q^f}$．从而 $\overline{G}=G(\overline{K}/\overline{k})=\langle\overline{\sigma}\rangle$是 f 阶循环群，而 $\overline{G}\cong G_{\mathfrak{P}}=G(K/K^d)$，$K^d$ 为 $\mathfrak{P}$ 的分解域．从而 $\overline{\sigma}$ 在 $G_{\mathfrak{P}}$ 有唯一原象 $\sigma=(\mathfrak{P},K/k)$，称为 $\mathfrak{P}$ 的 Frobenius 自同构．对于$\wp$的另一因子 $\mathfrak{P}_2=\tau\mathfrak{P}$，$(\mathfrak{P}_2,K/k)=\tau\sigma\tau^{-1}=\sigma$(见 § 3.6)，故 σ 只依赖于$\wp$，从而记为 $\sigma=\sigma_\wp=(\wp,K/k)$．由于 $\overline{\sigma}(\overline{a})=\overline{a}^q$，故 $\sigma_\wp$由下式唯一决定：

$$(\wp,K/k)\alpha\equiv\alpha^{N\wp}\pmod{\mathfrak{P}}\quad(\forall\ \alpha\in O_K).$$

因此每个非分歧素理想$\wp$对应一个$(\wp,K/k)\in G=G(K/k)$．这就得到(Artin)映射

$$\mathscr{A}:\ I(d)\longrightarrow G$$
$$\wp\longrightarrow(\wp,K/k),$$

其中 $d=\mathrm{Disc}(K/k)$，$\boldsymbol{I}(d)$是 k 中与 d 互素的分式理想全体，且 Artin 符号$(\wp,K/k)$按积性延拓到 $\boldsymbol{I}(d)$：

$$(\prod_i\wp_i,K/k)=\prod_i(\wp_i,K/k).$$

我们将证明 $\mathscr{A}$ 是满射，并确定 $\mathrm{Ker}\mathscr{A}$，从而得到基本定理：

$$I(d)/\mathrm{Ker}\mathscr{A}\cong G.$$

因 $\sigma_\wp$是 f 阶元，故若 $\mathfrak{Q}=N_{K/k}\mathfrak{P}=\wp^f$，则 $\mathscr{A}(\mathfrak{Q})=(\wp,K/k)^f=1$．故 $\mathrm{Ker}\mathscr{A}\supset N(d)=\{N_{K/k}(Q)\,|\,Q$ 为与 d 互素的 K 的理想$\}$．事实上，可证明 $\mathrm{Ker}\mathscr{A}=\boldsymbol{P}_dN(d)$，其中 $\boldsymbol{P}_d$ 是某些主理想．故有

$$\boldsymbol{I}(d)/\boldsymbol{P}_dN(d)\cong G.$$

我们还要考虑比 $\boldsymbol{I}(d)$更一般的广义理想群 $\boldsymbol{I}(\mathfrak{M})$；要使用 idele 群作为基本语言；要发展各基本定理；并给出局部—整体类域论的关系．

§9.1 Idele 群

设 k 为一数域，M_k 是其素除子集，其中 $\wp$-adic 素除子以 $\wp$ 记之. 设 k_v 是 k 对 $v\in M_k$ 的完备化. 直积

$$\prod_{v\in M_k} k_v$$

可以说含有 k 的全部信息. 但此集合显得太大，其中元素的性质与域的元素很不一样. 以 S_∞ 记无限素除子全体，U_v 是 k_v 的单位群.

定义 1 设 $a=(a_v)\in\prod_v k_v^*$，如果 a 的"几乎所有"分量 $a_v\in U_v$ 为单位，则 a 称为 k 的一个 idele("几乎所有"是指"除 S_∞ 和有限个之外全部"). 全体 idele 记为 J 或 J_k，称为 **idele 群**. 群运算为按分量相乘. k^* 按对角线嵌入 J，称为主 idele 群. 故有 $k^*\subset J$. $C_k=J/k^*$ 称为 **idele** 类群.

idele 源自 ideal element，是 Chevalley 1936 年提出的. 注意对于一个 idele $a=(a_v)$，它的有限个非单位分量是其本质.

设 $S\supset S_\infty$ 是 M_k 的一个有限子集，

$$J_S=\prod_{v\in S}k_v^*\times\prod_{v\notin S}U_v \tag{1}$$

中的元素称为 S-idele，其中 U_v 为 k_v 的单位群. 故 S-idele 就是只有 S-分量可以非单位的 idele. 显然

$$J=\bigcup_S J_S \tag{2}$$

而主 S-idele(或称 k^* 中 S-idele)群是指

$$k_S=k^*\cap J_S, \tag{3}$$

就是 S-单位群(§6.4 定理 2). 当 $S=S_\infty$ 时，k_S 即是普通单位群 $U(k)$.

注意 idele 群就是直积 $\coprod_v k_v^*$ 中只有"有限个分量"可非单位的元素集，不过这"有限个分量"应包含 S_∞-分量在内. 因此 $\boldsymbol{J}$ 也被称为 k_v^* ($v\in M_k$)的"限制直积". 注意 k_v^* 是局部紧群(即各点都有紧邻域，实则只需 1 有紧邻域). 例如当 v 是 $\wp$-adic 素除子时，由 §4.6 知 $1\in k_v^*$ 有一串紧邻域漏斗 $U_r=1+\wp^r=\{a\in k_v^* \mid \|a-1\|_v<(1/N\wp)^{r+1}\}$, $U_0=U_v$(见 §6.4)，即

$$k_v^*\supset U\supset U_1\supset U_2\supset\cdots\supset\{1\}.$$

故 $\boldsymbol{J}_S$ 是一些局部紧群的直积，而且"几乎所有"这些局部紧群(即 U_v)都是紧的. 所以 $\boldsymbol{J}_S$ 是局部紧群(对积拓扑). 我们令所有这些 $\boldsymbol{J}_S$ 为开集，随使 $\boldsymbol{J}$ 成为局部紧拓扑群. 事实上，下述即为 $1\in\boldsymbol{J}$ 的一个基本邻域系：

$$N(\varepsilon,S)=\left\{a=(a_v)\in\boldsymbol{J}\left|\begin{array}{ll}\|a_v-1\|_v<\varepsilon, & \text{当 } v\in S\\ \|a_v\|_v=1, & \text{当 } v\notin S\end{array}\right.\right\}\quad(4)$$

其中 S 过含 S_∞ 的素除子有限子集，$0<\varepsilon<1$ 任意. 所以，"a 很靠近 1"就意味着 a 的 S-分量很靠近 1(对所有 S)，也就意味着每个分量均很靠近 1. 同样，a 与 b 很靠近意味着每个分量均很靠近. 当然，上述基本邻域系也可改写为等价的基本邻域系：

$$\prod_{v\in S}W_v\times\prod_{v\notin S}U_v\quad(5)$$

其中 W_v 过 1 在 k_v^* 的基本邻域，$S\supset S_\infty$ 过素除子有限集. $1\in\boldsymbol{J}$ 的每个邻域含上述一个基本邻域，其闭包是紧的，故也可知 $\boldsymbol{J}$ 是局部紧群.

k^* 按对角线嵌入 $\boldsymbol{J}$，即对 $\alpha\in k^*$，将 α 等同于 $(\alpha,\alpha,\alpha,\cdots)\in\boldsymbol{J}$，于是 $k^*\subset\boldsymbol{J}$. 显然 k^* 是 $\boldsymbol{J}$ 的离散子群(从而也是闭子群). 事实上若 k^* 中元 $\alpha=(\alpha)\in N(1,S_\infty)$ 而 $\alpha\neq1=(1,1,\cdots)$，则 $\prod_v\|\alpha-1\|_v<1$ 与乘积公式矛盾(§6.4). 故邻域 $N(1,S_\infty)$

中只有 $1\in k_v^*$. 因此 idele 类群 $C_k=\boldsymbol{J}_k/k^*$ 仍为局部紧群.

设 K/k 是 n 次扩张, K 的 idele $a=(a_w)\in\boldsymbol{J}_K$ 的范 $N_{K/k}(a)$ 定义为 $b=(b_v)\in\boldsymbol{J}_k$, 其中

$$b_v=\prod_{w|v}N_w(a_w)\tag{6}$$

其中 N_w 表示 K_w 到 k_v 的(局部)范映射, 由 §4.8 知上述定义与 k^* 到 $\boldsymbol{J}$ 的嵌入相容, 即对 $\alpha\in K^*$, 作为元素的范的 idele $(N_{K/k}(\alpha)$, 等于主 idele (α)的范 $N_{K/k}(\alpha)$.

对 idele $a=(a_v)\in\boldsymbol{J}_k$, 定义 a 在 v 的标准赋值为 $\|a\|_v=\|a_v\|_v$, 定义 a 的体积为

$$\|a\|=\|a\|_k=\prod_{v\in M_k}\|a\|_v.\tag{7}$$

此乘积的几乎所有项为 1, 故乘积有意义. 体积为 1 的 idele 全体记为 $\boldsymbol{J}^0$. 乘积公式意味着 $k^*\subset\boldsymbol{J}^0$, 记 $C_k^0=\boldsymbol{J}_k^0/k^*$.

idele 的主要意义在于, 每个 idele $a=(a_v)\in\boldsymbol{J}$ 的有限除子分量决定一个理想

$$(a)=\prod_{v\notin S_\infty}\wp_v^{v(a_v)},\tag{8}$$

其中 $\wp_v$ 是 v 的赋值理想(常将 v 在 k_v 及 k 中的赋值理想用同一符号 $\wp_v$ 表示), $v(x)$表示 v 的标准指数赋值. 这就建立了 k 的 idele 群 $\boldsymbol{J}_k$ 到理想群 $\boldsymbol{I}_k=\boldsymbol{I}$ 的同态映射

$$\varphi:\ \boldsymbol{J}_k\longrightarrow\boldsymbol{I}_k,\qquad a\longrightarrow(a)\tag{9}$$

核恰为 S_∞-idele $\boldsymbol{J}_{S_\infty}$, 故

$$\boldsymbol{J}/\boldsymbol{J}_{S_\infty}\cong\boldsymbol{I}.\tag{10}$$

主理想子群 $\boldsymbol{P}\subset\boldsymbol{I}$ 在 φ 下的原象为 $k^*\boldsymbol{J}_{S_\infty}$, 故理想类群同构于

$$\boldsymbol{J}/k^*\boldsymbol{J}_{S_\infty}\cong\boldsymbol{I}/\boldsymbol{P}.\tag{11}$$

注意这是有限群，故可扩大 S_∞ 为 S 使 $\boldsymbol{J}_S$ 包含 $\boldsymbol{J}/k^*\boldsymbol{J}_{S_\infty}$ 中的所有陪集的代表元，则 $\boldsymbol{J}/k^*\boldsymbol{J}_S=1$. 所以存在有限集 $S\supset S_\infty$，使

$$\boldsymbol{J}=k^*\boldsymbol{J}_S,\quad C_k=k^*\boldsymbol{J}_S/k^*. \tag{12}$$

这也就是说，开子集 $\boldsymbol{J}_S$ 在 $\boldsymbol{J}$ 中是很大的. 而

$$\boldsymbol{J}/k^*\boldsymbol{J}_S\cong\frac{\boldsymbol{J}/k^*}{\boldsymbol{J}_S/k^*\cap\boldsymbol{J}_S}=\frac{C}{\boldsymbol{J}_S/k_S}=C/C_S. \tag{13}$$

其中 $C_S=\boldsymbol{J}_S/k_S$ 称为 S-idele 类群. 如果 $S=S_\infty$，上式右方即为 $\boldsymbol{I}/\boldsymbol{P}$，是有限群. 对一般的 S，因 $k^*\boldsymbol{J}_S\supset k^*\boldsymbol{J}_{S_\infty}$，故 C/C_S 是 $\boldsymbol{I}/\boldsymbol{P}$ 的同态象.

§9.2 射线理想类群

设 M_k 是域 k 的素除子集. 素除子的一个形式积

$$\mathfrak{M}=\prod_{v\in M_k}v^{m(v)}=\prod_v\mathfrak{M}_v$$

称为一个除子(divisor)，其中 $m(v)\in\boldsymbol{Z}$ 只对有限多个 v 非 0，$\mathfrak{M}_v=v^{m(v)}$ 称为 m 的 v-分量. 满足下列条件的除子 $\mathfrak{M}$ 称为**模**(modulus)**或闭链**(cycle)：$\mathfrak{M}(v)\geqslant 0$ 且

$$m(v)=\begin{cases}0\text{ 或 }1, & \text{当 } v \text{ 为实素除子.}\\ 0, & \text{当 } v \text{ 为复素除子.}\end{cases}$$

也就是说，模 $\mathfrak{M}$ 不含复素除子，每个实素除子最高只能一次. 记 $\mathfrak{M}=\mathfrak{M}_0\mathfrak{M}_\infty$，其中 $\mathfrak{M}_0=\prod_{v\nmid\infty}v^{m(v)}=\prod_{\wp\nmid\infty}\wp^{m(v)}$ 可等同于一个理想，称为 $\mathfrak{M}$ 的有限部分，$\mathfrak{M}_\infty=\prod_{v\mid\infty}v^{m(v)}$ 是无限部分. 若 $v\mid\mathfrak{M}_0$ 是非阿基米德素除子，常以 $\wp_v$ 记其赋值素理想.

定义 1 对 $a=(a_v)\in\boldsymbol{J}_k$,定义

$$a\equiv 1\ (\mathrm{mod}^*\,\mathfrak{M})$$

意义为

$$a_v\equiv 1\ (\mathrm{mod}^*\,\mathfrak{M}_v)\quad(\text{所有 } v|\mathfrak{M})$$

即

$$a_v\in W_{\mathfrak{M}}(v)=\begin{cases}1+\wp^{m(v)}, & \text{当 } \wp\,|\,\mathfrak{M}_0;\\ \boldsymbol{R}^+\ (\text{正实数}), & \text{当 } v\,|\,\mathfrak{M}_\infty \text{ 为实除子}.\end{cases}$$

满足 $a\equiv 1(\mathrm{mod}^*\,\mathfrak{M})$的 $a\in\boldsymbol{J}$ 全体记为 $\boldsymbol{J}_{\mathfrak{M}}$,记 $k_{\mathfrak{M}}=k^*\cap\boldsymbol{J}_{\mathfrak{M}}$.

显然

$$J_{\mathfrak{M}}=\prod_{v|\mathfrak{M}}W_{\mathfrak{M}}(v)\times\prod_{v\nmid\mathfrak{M}}{}'k_v^*$$

(其中 $\prod'$ 表示只有限个分量(包含无限素除子分量)可以不是局部单位).为了记号方便,当 v 是无限素除子时,常记 $U_v=k_v^*$.当 $v\nmid\mathfrak{M}$ 时,记 $W_{\mathfrak{M}}(v)=U_v$.并记

$$W_{\mathfrak{M}}=\prod_{v|\mathfrak{M}}W_{\mathfrak{M}}(v)\times\prod_{V\nmid\mathfrak{M}}U_v.$$

显然,$W_{\mathfrak{M}}$ 全体形成 $\boldsymbol{J}$ 的含 1 开子群的一个基本系.也就是说,每个 $\boldsymbol{W}_{\mathfrak{M}}$ 是开的,而且任给 $\boldsymbol{J}$ 的含 1 开子群,总存在某 $\mathfrak{M}$ 使此子群含 $W_{\mathfrak{M}}$.

k^* 中满足 $a\equiv 1(\mathrm{mod}^*\,\mathfrak{M})$的元素 α 全体为 $k_{\mathfrak{M}}=k^*\cap\boldsymbol{J}_{\mathfrak{M}}$,所有这种 α 生成的主理想(α)全体记为 $\boldsymbol{P}_{\mathfrak{M}}$,以 $\boldsymbol{I}(\mathfrak{M})$记与 $\mathfrak{M}$ 互素的 k 的分式理想 $\boldsymbol{I}$ 全体(即 $\boldsymbol{I}$ 分解为素理想幂之积后,分子分母中的素理想均不含于 $\mathfrak{M}$.).称

$$\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}$$

为 k 的**射线理想类群**(ray ideal class group)或 $\mathfrak{M}$-理想类群.其中元素个数记为 $h_{\mathfrak{M}}$,称为射线理想类数,或 $\mathfrak{M}$-理想类数.

现考虑 $\boldsymbol{I}(\mathfrak{M})/\mathbf{P}_{\mathfrak{M}}$ 与普通理想类群 $\boldsymbol{I}/\boldsymbol{P}$ 的关系. 首先易知, $\boldsymbol{I}/\boldsymbol{P}$ 中每个理想类均含有 $\boldsymbol{I}(\mathfrak{M})$中的整理想. 事实上,在 $\boldsymbol{I}/\boldsymbol{P}$ 的给定类中任取一整理想 $\boldsymbol{I}$,由孙子定理(中国剩余定理)知有 $\alpha\in O_k$ 使

$$\alpha\equiv\pi_v^{v(I)}\qquad(\bmod\ \wp_v^{v(I)+1}),\quad v\mid\mathfrak{M}.$$

(其中 $\pi_v\in\wp_v-\wp_v^2$, $\wp_v^{v(I)}\parallel I$). 于是 $\alpha^{-1}I$ 与 $\mathfrak{M}$ 互素. 再求 $\beta\in O_k$,使 $\beta\equiv1(\bmod\ \wp_v)$(所有 $v\mid\mathfrak{M}$), $\beta\equiv\pi_v^{-v(\alpha^{-1}I)}(\bmod\ \wp_v^{-v(\alpha^{-1}I)+1})$(当 $v\nmid\mathfrak{M}$, $v(\alpha^{-1}I)<0$),则 $\alpha^{-1}\beta I$ 为 $\boldsymbol{I}(\mathfrak{M})$中整理想. 这说明 $\boldsymbol{I}(\mathfrak{M})$在模 $\boldsymbol{P}_{\mathfrak{M}}$ 同态下的象为整个理想类群 $\boldsymbol{I}/\boldsymbol{P}$,记

$$\boldsymbol{P}(\mathfrak{M})=\boldsymbol{P}\cap\boldsymbol{I}(\mathfrak{M})$$

为与 $\mathfrak{M}$ 互素的主理想全体,则有

$$\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}(\mathfrak{M})\cong\boldsymbol{I}/\boldsymbol{P}.$$

而 $\boldsymbol{P}(\mathfrak{M})$由 $k(\mathfrak{M})$生成,$k(\mathfrak{M})$是与 $\mathfrak{M}$ 互素的 k 中数集. 而生成 $\boldsymbol{P}_{\mathfrak{M}}$ 的全体数是 $Uk_{\mathfrak{M}}$,$U=U(k)$是 k 的单位群. 从而 $\boldsymbol{P}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}\cong k(\mathfrak{M})/Uk_{\mathfrak{M}}$.

$$\begin{array}{ccccc}
 & & & & \boldsymbol{I}(\mathfrak{M}) & \longrightarrow & \boldsymbol{I}\\
 & & & & \mid h & & \mid h\\
 & & k(\mathfrak{M}) & \longrightarrow & \boldsymbol{P}(\mathfrak{M}) & \longrightarrow & \boldsymbol{P}\\
 & & \mid i & & \mid i & & \\
U & \longrightarrow & Uk_{\mathfrak{M}} & \longrightarrow & \boldsymbol{P}_{\mathfrak{M}} & & \\
\mid j & & \mid j & & & & \\
U_{\mathfrak{M}} & \longrightarrow & k_{\mathfrak{M}} & & & &
\end{array}$$

$Uk_{\mathfrak{M}}/k_{\mathfrak{M}}\cong U/k_{\mathfrak{M}}\cap U=U/U_{\mathfrak{M}}$,$U_{\mathfrak{M}}$ 是 $\bmod^*\mathfrak{M}$ 为 1 的 k 单位集. 故

$$h_{\mathfrak{M}}=\#\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}=(\#\boldsymbol{I}(\mathfrak{M})/\mathbf{P}(\mathfrak{M}))(\#\mathbf{P}(\mathfrak{M})/\mathbf{P}_{\mathfrak{M}})$$

$$=(\# \mathbf{I}/\mathbf{P})(\# k(\mathfrak{M})/Uk_{\mathfrak{M}})$$

$$=h(k(\mathfrak{M}):k_{\mathfrak{M}})/(U:U_{\mathfrak{M}}).$$

而 $k(\mathfrak{M})/k_{\mathfrak{M}}$ 有类似孙子定理的分解：

$$k(\mathfrak{M})/k_{\mathfrak{M}} \cong \coprod_{v|\mathfrak{M}_0}(O_v/\wp_v^{m(v)})^* \times \prod_{\text{实}v|\mathfrak{M}_\infty}\mathbf{R}^*/\mathbf{R}^+ \qquad (*)$$

每个 $\alpha\in k(\mathfrak{M})(\bmod k_{\mathfrak{M}})$ 对应于它的各局部剩余类(其中 R^* 表示环 R 的单位群，$\mathbf{R}^+$是正实数乘法群). 事实上，$k(\mathfrak{M})$到上式右方有自然同态 φ，由逼近定理(§4.4)知 φ 是满射，显然 $\mathrm{Ker}\varphi=k_{\mathfrak{M}}$，即知有上述同构. 这提示我们定义 Euler 函数

$$\varphi(\mathfrak{M}) = \prod_{v|\mathfrak{M}_0}\#(O_v/\wp_v^{m(v)})^* \cdot 2^{\#\mathfrak{M}_\infty} = (k(\mathfrak{M}):k_{\mathfrak{M}}).$$

显然 $\varphi(v^m)=(N\wp_v-1)N\wp_v^{m-1}$. 我们证明了

定理 1 数域 k 的射线理想类数 $h_{\mathfrak{M}}=\# \boldsymbol{I}(\mathfrak{M})/\mathbf{P}_{\mathfrak{M}}$ 等于

$$h_{\mathfrak{M}} = \frac{h\varphi(\mathfrak{M})}{(U:U_{\mathfrak{M}})}$$

是有限数，其中 h 是 k 的理想类数.

注记 1 $(U:U_{\mathfrak{M}})$有限，故 $U_{\mathfrak{M}}$ 也有 $r=r_1+r_2-1$ 个独立单位作为生成元，设为 $\varepsilon_1,\cdots,\varepsilon_r$(不计单位根). 则可定义 $\mathfrak{M}$-正规子 $R_{\mathfrak{M}}$ 为

$$R_{\mathfrak{M}} = |\det(\log|\sigma_i\varepsilon_j|^{n_i})|(1\leqslant i,j\leqslant r).$$

例 1 设 $\mathfrak{M}=1$，则 $\boldsymbol{I}(\mathfrak{M})=\boldsymbol{I}$，$\boldsymbol{P}_{\mathfrak{M}}=\boldsymbol{P}$，$h_{\mathfrak{M}}=h$.

例 2 设 $k=\boldsymbol{Q}$，$\mathfrak{M}=m\infty$(其中 m 为自然数，是一些素数(素除子)的积). 则 $\varphi(\mathfrak{M})=2\varphi(m)$. 因 $U=\{\pm1\}$，故 $U_{\mathfrak{M}}=\{1\}$(因$\infty|\mathfrak{M}$，故 $u\equiv1(\bmod^*\mathfrak{M})$要求 $u=u_\infty\in W_\infty=\boldsymbol{R}^+$，故 $u>0$).

从而 $h_{\mathfrak{M}}=2\varphi(m)/2=\varphi(m)$. $Q_{\mathfrak{M}}$ 由满足 $\alpha\equiv 1(\bmod m)$ 的正有理数组成. 在上述广义孙子分解(*)式中, $(O_v/\wp_v^{m(v)})^*\cong(\mathbf{Z}/p^{m(v)}\mathbf{Z})^*$, 从而 $k(\mathfrak{M})/k_{\mathfrak{M}}\cong(\mathbf{Z}/m\mathbf{Z})^*\times\{1,-1\}$, 故 $\boldsymbol{I}(\mathfrak{M})/\mathbf{I}_{\mathfrak{M}}\cong(\mathbf{Z}/m\mathbf{Z})^*$. 故每一个 $\mathfrak{M}$-理想类可看作是与 m 互素的一个算术级数.

如果取 $k=Q$ 而 $\mathfrak{M}=m$, 则 $U_m=U$, $h_m=\varphi(m)/2$. $k(m)/k_m\cong(\mathbf{Z}/m\mathbf{Z})^*$, $\boldsymbol{I}(m)/\mathbf{P}_m\cong(\mathbf{Z}/m\mathbf{Z})^*/\{1,-1\}$.

对 $k=\mathbf{Q}$ 取 $\mathfrak{M}=\infty$, 则 k_∞ 是正有理数全体, 在几何上是一"射线". 这就是射线理想类名词的由来.

一般地, 由广义孙子分解(*)式可知, $k(\mathfrak{M})/k_{\mathfrak{M}}$ 的 $\varphi(\mathfrak{M})$ 个陪集可如下表示

$$k(\mathfrak{M})=\{\alpha_1\cup\cdots\cup\alpha_r\}\cdot\{\beta_1\cup\cdots\cup\beta_S\}\cdot k_{\mathfrak{M}},$$

其中 $\{\alpha_i\in O_k\}$ 是 $(O_k/\mathfrak{M}_0)^*$ 的 $r=\varphi(\mathfrak{M}_0)$ 个代表元, $\{\beta_j\in O_k\}$ 在各实素除子 $v|\mathfrak{M}_\infty$ 上的符号恰为所有 $s=2^{\#\mathfrak{M}_\infty}$ 种可能排列. (当然我们可以选取 α_i 使它在 $v|\mathfrak{M}_\infty$ 为正数, 可取各 β_j 使 $\beta_j\equiv 1 \bmod^* \mathfrak{M}_0$)(在表达式 $O_k/\mathfrak{M}_0$ 中是将 $\mathfrak{M}_0$ 等同于理想).

例 3 设 $k=Q(\sqrt{d})$ 为实二次域. $\mathfrak{M}=\infty_1\infty_2=\infty$ 这里 ∞_1 和 ∞_2 是 k 的仅有两个实素除子. 按定理 1 有 $h_\infty=h2^2/(U:U_\infty)$. 设 $\varepsilon>1$ 是 k 的基本单位, 则 $U=\pm\varepsilon^{\mathbf{Z}}$. 若 $N(\varepsilon)=\varepsilon\bar{\varepsilon}=-1$, 则 $|\varepsilon|_{\infty_2}=\bar{\varepsilon}<0$, 故 $\varepsilon\notin U_\infty$. 从而 $U_\infty=\varepsilon^{2\mathbf{Z}}$. 即知 $(U:U_\infty)=4$, $h_\infty=h$. 当 $N(\varepsilon)=1$ 时, $\varepsilon\in U_\infty$, 故 $U_\infty=\varepsilon^{\mathbf{Z}}$, $(U:U_\infty)=2$, $h_\infty=2h$. 即

$$h_\infty=\begin{cases}h, & \text{若 } N(\varepsilon)=-1.\\ 2h, & \text{若 } N(\varepsilon)=1.\end{cases}$$

注意 $\boldsymbol{I}=I(\infty)$ 中两理想 I 与 J 对模 $\boldsymbol{P}_\infty$ 在同一类(称为 ∞-等价)

当且仅当

$$I = J(\alpha),$$

其中 $\alpha \in k$ 且 $N(\alpha) > 0$（即 $(\alpha) \in \boldsymbol{P}_\infty$ 或 $\alpha \in k_\infty$，亦即 α 在 ∞_1 和 ∞_2 取值皆正）. 这就是 §7.3.1 中定义的**严义等价**. $h_\infty = h^+$ 就是**严义类数**. $k(\infty)/k_\infty$ 的代表元可取为 $\{1, -1, \sqrt{d}, -\sqrt{d}\}$（即上述 $\{\beta_j\}$），故 $\boldsymbol{I}(\infty)/\boldsymbol{P}_\infty$ 的代表元 $\subset \{(1), (\sqrt{d})\}$. 当且仅当 $N(\varepsilon) = -1$ 时 $(\sqrt{d}) = (\varepsilon\sqrt{d})) \in \boldsymbol{P}_\infty$，从而 $h_\infty = h$；否则 $h_\infty = 2h$.

□

现设 k 为 n 次数域，$\mathfrak{M}$ 为其一模，B 是 $\boldsymbol{I}(\mathfrak{M})/\mathbf{P}_\mathfrak{M}$ 中一个射线理想类. 记 $j(B,t)$ 为满足 $NI \leqslant t$ 的 B 中整理想 I 的个数，则可证明：

$$j(B,t) = \rho_\mathfrak{M} t + O(t^{1-1/n}).$$

其中

$$\rho_\mathfrak{M} = \frac{2^{r_1}(2\pi)^{r_2} R_\mathfrak{M}}{W_\mathfrak{M}\sqrt{d_k} N(\mathfrak{M})}.$$

这里 $R_\mathfrak{M}$ 是 $\mathfrak{M}$-正规子（见注记 1），$N(\mathfrak{M}) = N(\mathfrak{M}_0) 2^{\#\mathfrak{M}_\infty}$（视 $\mathfrak{M}_0$ 为理想），$W_\mathfrak{M}$ 是 $U_\mathfrak{M}$ 中单位根个数，d_k 是 k 判别式的绝对值. 上式的证明是用 k 到 $\boldsymbol{R}^n$ 的嵌入，计算凸区域中的格点数（[La]）.

§9.3 理想类群与伊代尔类群

设 k 为数域，$\mathfrak{M}$ 是其一模，$\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_\mathfrak{M}$ 为其一射线类群，$\boldsymbol{J} = \boldsymbol{J}_k$ 为其 Idele 群. 每个 idele $a \in \boldsymbol{J}$ 决定一个理想 $(a) \in \boldsymbol{I} = \boldsymbol{I}_k$. 若 $(a) \in \boldsymbol{I}(\mathfrak{M})$，即与 $\mathfrak{M}$ 互素，则 (a) 只有 $v \nmid \mathfrak{M}$ 的分量. 由此知下列同态是满射：

$$\psi: \boldsymbol{J}_{\mathfrak{M}} \longrightarrow \boldsymbol{I}(\mathfrak{M}),\ a \longrightarrow (a),$$

其中的 $\boldsymbol{J}_{\mathfrak{M}}$ 由满足 $a \equiv 1(\bmod^* \mathfrak{M})$（即 $a_v \equiv 1 \bmod^* \mathfrak{M}_v$，亦即 $a_v \in W_{\mathfrak{M}}(v)$，$v|\mathfrak{M}$）的 idele a 组成. 显然

$$W_{\mathfrak{M}} := \operatorname{Ker}\psi = \prod_{v|\mathfrak{M}} W_{\mathfrak{M}}(v) \times \prod_{v \nmid \mathfrak{M}} U_v$$

（当 v 为无限素除子时 $U_v = k_v^*$），$\boldsymbol{P}_{\mathfrak{M}} \subset \boldsymbol{I}(\mathfrak{M})$ 的全原象显然为 $k_{\mathfrak{M}} W_{\mathfrak{M}}$，故得

$$\boldsymbol{J}_{\mathfrak{M}} / k_{\mathfrak{M}} W_{\mathfrak{M}} \cong \boldsymbol{I}(\mathfrak{M}) / \boldsymbol{P}_{\mathfrak{M}} \tag{1}$$

注意 $\{W_{\mathfrak{M}}\}$ 构成 $\boldsymbol{J}$ 中开子群在 1 的基本开子集系，我们以 $W_{\mathfrak{M}}(v)$ 记 $W_{\mathfrak{M}}$ 的 v-分量（即当 $v \nmid \mathfrak{M}$ 时记 $W_{\mathfrak{M}}(v) = U_v$）.

(1)式将射线理想类群表示成了 idele 的一个类群. 当 $k = \boldsymbol{Q}$，$\mathfrak{M} = m\infty$ 时，(1)式右方为 $(\boldsymbol{Z}/m\boldsymbol{Z})^* = G_m$（上节例 2），同构于 $L_m = \boldsymbol{Q}(\zeta_m)$ 的 Galois 群. 这是类域论的主要思路的一个特别情形：k 的理想类群 $\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_m$ 同构于它的 Abel 扩张 L_m/k 的 Galois 群. 如果 $K/k \subset L_m/k$，则 $G(K/k)$ 是 G_m 的商群. 将会证明

$$G(K/k) \cong \boldsymbol{J}_k / k^* N_{K/k} \mathbf{J}_K,$$

与(1)式对照即知，应有 $W_{\mathfrak{M}} \subset N\boldsymbol{J}_K$. 也就是说，给定 K/k，寻求 $\mathfrak{M}$ 使 $K \subset L_m$ 约相当于寻求 $\mathfrak{M}$ 使 $W_{\mathfrak{M}} \subset N\boldsymbol{J}_K$. 这即是下述定义的原因.

定义 1 设 K/k 是 n 次 Galois 扩张，$\mathfrak{M}$ 是 k 的模. 称 $\mathfrak{M}$ 对 K/k 是**可许模**(admissible modulus)是指 $W_{\mathfrak{M}} \subset N_{K/k}\boldsymbol{J}_K$，亦即

$$W_{\mathfrak{M}}(v) \subset N_w K_w^* \qquad (\text{所有 } w|v \in M_k).$$

最小(按除法)可许模记为 $\mathfrak{f}(K/k)$，称为**导子**.

这里 w 是 v 到 K 的延拓，K_w 是 K 对 w 的完备化，N_w 是 K_w 到 k_v 的范映射. 显然 $U_v \cap N_w K_w^* = N_w U_w$，故 $U_v \subset N_w K_w^* \Leftrightarrow$

$U_v=N_wU_w$. 将在 § 9.6 证明$(U_v : N_wU_w)=e(w|v)$. 故 v 在 K 非分歧$\Leftrightarrow v\nmid F$，也就是说，$F(K/k)$含且仅含分歧素除子(注意，当 v 为无限素除子时，w 对 v 非分歧规定为 $K_w=k_v$. 即仅当 v 实而 w 虚时称为分歧). 令

$$\mathscr{N}(\mathfrak{M})=\{N_{K/k}I \mid I \text{ 为与 } \mathfrak{M} \text{ 互素的 } K \text{ 的理想}\}.$$

定理 1 设 F 为 K/k 的导子(最小可许模)，$\mathfrak{M}$ 为可许模(即 $F|\mathfrak{M}$)，则

(i) $I(\mathfrak{M})/P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})\cong I(\mathfrak{f})/P_{\mathfrak{f}}\mathscr{N}(F)$.

(ii) $P_{\mathfrak{f}}\mathscr{N}(F)\cap I(\mathfrak{M})=P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$；

$P_{\mathfrak{f}}\mathscr{N}(F)=P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$(当 $\mathfrak{M}$ 与 f 素因子相同).

证明 先证(ii)第 1 式，设 $I\in$ 左式，则有 $I\in I(\mathfrak{M})$且 $I=(\alpha)N(J)$，$\alpha\in k_{\mathfrak{f}}$，$J\in I(K)$与 F 互素.

(a) 设 $w|v$，$v|F$. 则 $\alpha=\alpha_v\subset W_{\mathfrak{f}}(v)\subset N_wK_w^*$，故 $\alpha=N_w\gamma_w$，$\gamma_w\in K_w^*$. 因 $\alpha_v=\alpha\in k_{\mathfrak{f}}$ 是 v-单位，故 γ_w 可取为 w-单位. 由赋值的逼近定理，可取 $\gamma\in K$ 使

$$\begin{cases} N\gamma\approx\alpha & (\text{对所有 } v|f) \\ w(\gamma)=-w(J) & (\text{对 } w|v, v|\mathfrak{M}, v\nmid \mathfrak{f}) \end{cases}$$

(事实上，可取 γ 使对每个 $v|f$ 恰在一个 $w|v$ 处 γ 近于 γ_w，在其余 $w'|v$ 处 γ 近于 1，则 $N\gamma$ 的 v-分量为 $\prod\limits_{w|v}N_w\gamma\approx N_u\gamma_u=\alpha$).

于是有

$$\begin{cases} \alpha N\gamma^{-1}\approx 1 & (v|f) \\ \gamma J \text{ 与 } \mathfrak{M} \text{ 互素} \end{cases}$$

(在 $\mathfrak{M}/F$ 为单位，在 F 近于 α，故与 F 互素). 从而

$$I=(\alpha)N(J)=(\alpha N\gamma^{-1})N(\gamma J).$$

(b)因 $I\in \boldsymbol{I}(\mathfrak{M})$ 与 $\mathfrak{M}$ 互素，故 $I=(\alpha)N(J)$ 在 $\mathfrak{M}/\boldsymbol{F}$ 各位上为单位. 而 γJ 也为单位，即知 $N(\gamma)N(J)$ 为单位，故 $\alpha N(\gamma^{-1})$ 为单位(在 $\mathfrak{M}/\boldsymbol{F}$)，从而 $\beta=\alpha N(\gamma^{-1})$ 在 $v|\mathfrak{M}$ 为单位(因在 $v|\boldsymbol{f}$ 近于 1)，且

$$\beta=\beta_v=N_w\delta_w(\text{对 } v|\mathfrak{M}/\boldsymbol{F}),\delta_w\in K_w^*,$$

(因由 $\boldsymbol{F}$ 的定义知，当 $v\nmid \boldsymbol{F}$ 时应有 $U_v=W_f(v)\subset N_wK_w^*$). 从而可如上再用逼近定理，取 $\gamma_1\in K$ 使

$$\begin{cases} N\gamma_1\approx\beta & (\text{对 } v|\mathfrak{M}/\boldsymbol{F}) \\ \gamma_1\approx 1 & (\text{对 } v|\boldsymbol{F}) \end{cases}$$

则 $\beta N\gamma_1^{-1}\approx 1\ (v|\mathfrak{M})$. 特别 $\beta N\gamma_1^{-1}\equiv 1(\bmod{}^*\mathfrak{M})$，而 $I=(\beta)N(\gamma J)=(\beta N\gamma_1^{-1})N(\gamma\gamma_1 J)\in \boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$.

这就证明了(ii)，(i)显然可知. □

$\boldsymbol{k}$ 的每个 idele a 决定了它的一个理想(a)，从而引起满同态 ψ: $\boldsymbol{J}\supset \boldsymbol{J}_{\mathfrak{M}}\longrightarrow \boldsymbol{I}(\mathfrak{M})$，核为 $W_{\mathfrak{M}}$，$\boldsymbol{P}_{\mathfrak{M}}$ 的原象为 $k_{\mathfrak{M}}W_{\mathfrak{M}}$. 通过这一映射我们将可以看到 idele 的很好的性质. 不仅 idele 可以象理想那样运算，而且各种理想子群(如:范子群)和类群与相应的 idele 的子群和类群均有很自然的对应. 考虑下图中理想子群与 idele 子群的对应(记号见定义 1 和定理 1)：

$$\begin{array}{ccccc}
\boldsymbol{J} & \xleftarrow{\ i\ } & \boldsymbol{J}_{\mathfrak{M}} & \xrightarrow{\ \psi\ } & \boldsymbol{I}(\mathfrak{M}) \\
| & & | & & | \\
k^*N\boldsymbol{J}_K & \xleftarrow{\ i\ } & \psi^{-1}(\boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})) & \xrightarrow{\ \psi\ } & \boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M}) \\
| & & | & & | \\
k^*W_{\mathfrak{M}} & \xleftarrow{\ i\ } & k_{\mathfrak{M}}W_{\mathfrak{M}} & \xrightarrow{\ \psi\ } & \boldsymbol{P}_{\mathfrak{M}}
\end{array}$$

图中 ψ: $a\longrightarrow(a)$ 为 idele 到理想的映射，i 为包含映射，竖线为包含关系，参见(1)式. ψ 均为满射，i 均为单射.

引理 1 设 K/k 为有限扩张，$\mathfrak{M}$ 是 K/k 的可许 k-模，则

(1) $\psi^{-1}(P_{\mathfrak{M}}\mathcal{N}(\mathfrak{M}))=k_{\mathfrak{M}}W_{\mathfrak{M}}N\boldsymbol{J}_K(1,\mathfrak{M})$,
其中 $\boldsymbol{J}_K(1,\mathfrak{M})$ 为 $w|\mathfrak{M}$ 分量为 1 的 K 的 idele 集.

(2) $\psi^{-1}(P_{\mathfrak{M}}\mathcal{N}(\mathfrak{M}))=k^*N\boldsymbol{J}_k\cap\boldsymbol{J}_{\mathfrak{M}}$.

证明 (1)设 $a\in\boldsymbol{J}_{\mathfrak{M}}$ 使 $(a)\in P_{\mathfrak{M}}\mathcal{N}(\mathfrak{M})$,记 $(a)=\alpha N(I)$. 取 $A\in\boldsymbol{J}_k$ 与 I 的分量阶均相同(即当 $\mathfrak{P}_w|I$ 时,$w(A_w)=w(I)$),A 的其余($\mathfrak{P}_w\nmid I$ 时)分量均为 1. 则 $N(A)=N(I)$,$A\in\boldsymbol{J}_K(1,\mathfrak{M})$,$(a)=(\alpha NA)$. 故 a 与 αNA 相差一个 $W_{\mathfrak{M}}$ 中元(处处为单位,且在 $\mathfrak{M}$ 分量受限于 $a\in\boldsymbol{J}_{\mathfrak{M}}$,$\alpha\in k_{\mathfrak{M}}$,$A=1$),故 $a\in k_{\mathfrak{M}}W_{\mathfrak{M}}N\boldsymbol{J}_K(1,\mathfrak{M})$,另一方向包含关系显然.

(2) 因 $\mathfrak{M}$ 为可许模,故 $W_{\mathfrak{M}}\subset N\boldsymbol{J}_K$,从而 $k_{\mathfrak{M}}W_{\mathfrak{M}}N\boldsymbol{J}_K(1,\mathfrak{M})\subset k^*N\boldsymbol{J}_K\cap\boldsymbol{J}_{\mathfrak{M}}$. 反之,若 $a\in k^*N\boldsymbol{J}_K\cap\boldsymbol{J}_{\mathfrak{M}}$,设 $a=\alpha NA\in\boldsymbol{J}_{\mathfrak{M}}$,设 $A=\beta\dfrac{B}{\beta}\dfrac{A}{B}$,其中 $\beta\in k$ 在 $v|\mathfrak{M}$ 近于 A; $B\in\boldsymbol{J}_K$ 在 $v|\mathfrak{M}$ 与 A 同,其余分量与 β 同,则 $A/B\in\boldsymbol{J}_K(1,\mathfrak{M})$. 故 $a=(\alpha)(N\beta)(NB/\beta)(NA/B)\in k_{\mathfrak{M}}W_{\mathfrak{M}}N\boldsymbol{J}_K(1,\mathfrak{M})$. □

定理 2 设 K/k 为 n 次扩张,$\mathfrak{M}$ 是 k 的模,对 K/k 是可许的. 设 ψ: $\boldsymbol{J}\longmapsto\boldsymbol{I}$, $a\longmapsto(a)$, 将 k 的 idele 自然地映为理想,ψ 诱导出的各种映射记为 ψ_i. 设 φ: $\boldsymbol{J}/k^*\longmapsto\boldsymbol{J}_{\mathfrak{M}}/k_{\mathfrak{M}}$,$\bar{a}\longmapsto\bar{b}$ 为自然同构,φ 诱导出的各种映射记为 φ_i. 则有下列交换图,其中横行均为群同构,竖列均为自然群同态:

$$\begin{array}{ccccc}
C=\boldsymbol{J}/k^* & \xrightarrow{\varphi} & \boldsymbol{J}_{\mathfrak{M}}/k_{\mathfrak{M}} & & \\
\downarrow & & \downarrow & & \\
\boldsymbol{J}/k^*W_{\mathfrak{M}} & \xrightarrow{\varphi_1} & \boldsymbol{J}_{\mathfrak{M}}/k_{\mathfrak{M}}W_{\mathfrak{M}} & \xrightarrow{\Psi_1} & \boldsymbol{I}(\mathfrak{M})/P_{\mathfrak{M}} \\
\downarrow & & \downarrow & & \\
C/NC_K\overset{\sigma}{\cong}\boldsymbol{J}/k^*N\boldsymbol{J}_K & \xrightarrow{\varphi_2} & \boldsymbol{J}_{\mathfrak{M}}/k_{\mathfrak{M}}W_{\mathfrak{M}}N\boldsymbol{J}_K(1,\mathfrak{M}) & \xrightarrow{\Psi_2} & \boldsymbol{I}(\mathfrak{M})/P_{\mathfrak{M}}\mathcal{N}(\mathfrak{M})
\end{array}$$

证明 (1) ψ_1 是同构,见本节(1)式.

(2) ψ_2 是同构,见本节引理 1(1).

(3) φ是同构,是因 $\boldsymbol{J}/k^*$ 中每个类中都有 $\boldsymbol{J}_{\mathfrak{M}}$ 中元(对任意 $a\in\boldsymbol{J}$,由逼近定理知,存在 $\alpha\in k^*$ 使 $\alpha=a_v(v|\mathfrak{M}$ 时),于是 $\alpha^{-1}a\in\boldsymbol{J}_{\mathfrak{M}}$),亦即 $\boldsymbol{J}=k^*\boldsymbol{J}_{\mathfrak{M}}$,而 $k_{\mathfrak{M}}=k^*\cap\boldsymbol{J}_{\mathfrak{M}}$. 故

$$\boldsymbol{J}/k^*=\boldsymbol{J}_{\mathfrak{M}}k^*/k^*=\boldsymbol{J}_{\mathfrak{M}}/k_{\mathfrak{M}}.$$

(4) φ_1 是同构,原因与 φ 相同.

(5) φ_2 是同构,由本节引理 1(2), $k^*N\boldsymbol{J}_K\cap\boldsymbol{J}_{\mathfrak{M}}=k_{\mathfrak{M}}W_{\mathfrak{M}}N\boldsymbol{J}_K(1,\mathfrak{M})$.

(6) σ 是同构,见§9.1 中(13)式.

上述定理将理想类群与 idele 类群统一了起来(注意 C/NC_K,$\boldsymbol{J}/K^*N\boldsymbol{J}_K$均与模 $\mathfrak{M}$ 无关). 以下是要证明这些类群与 Galois 群同构,即开始证明类域论的主定理.

当 $k=\boldsymbol{Q}$,$\mathfrak{M}=m\infty$时,如§9.2 例 2 可知,类群 $\boldsymbol{J}/k^*W_m\cong\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}\cong(\boldsymbol{Z}/m\boldsymbol{Z})^*$,即同构于分圆域 $\boldsymbol{Q}(\zeta_m)$的 Galois 群;故子群 $\boldsymbol{P}_{\mathfrak{M}}$(或 $k^*W_{\mathfrak{M}}$)对应于 $\boldsymbol{Q}(\zeta_m)$. 而若 $K\subset\boldsymbol{Q}(\zeta_m)$(即若 $\mathfrak{M}$ 是 $K/\boldsymbol{Q}$ 的可许模),则类群 $\boldsymbol{J}/k^*N\boldsymbol{J}_K\cong\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$ 是$(\boldsymbol{Z}/m\boldsymbol{Z})^*$ 的商群,同构于 $G(K/\boldsymbol{Q})$(将证明);故子群 $\boldsymbol{P}_m\mathscr{N}(\mathfrak{M})$对应于 $K\subset\boldsymbol{Q}(\zeta_{\mathfrak{M}})$.

为了证明类域论主定理,即类群同构于 Galois 群:

$$\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})\cong G(K/k),$$

将先证明它们的阶(元素个数)$h=n$. 然后(或同时)用 Artin 映射给出同构对应. h 称为类数(广义的或射线的——后者特别对 $\mathscr{N}(\mathfrak{M})\subset\boldsymbol{P}_{\mathfrak{M}}$ 情形),也称为**范指数**,将先证明第二和第一范指数不等式:$h\leqslant n$, $h\geqslant n$.

§9.4 通用范指数不等式

首先需讨论 Hecke L-函数等解析理论，将上章理论稍作发展.

设 k 为 n_0 次数域，$\mathfrak{M}$ 是其一模，$B\in \boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}$ 是其一射线理想类，定义

$$\zeta_k(s,\mathfrak{M},B)=\sum_{I\in B}\frac{1}{NI^s}.$$

其中 I 过 B 中整理想，记 $\zeta_k(s,\mathfrak{M},B)=\sum_{i=1}^{\infty}\frac{a_i}{i^s}$，则 $A_i=a_1+\cdots+a_i=\#\{I\in B\mid NI\leqslant i\}=j(B,i)=\rho_{\mathfrak{M}}i+O(i^{1-1/n_0})$（见 §9.2 最后）. 由 §8.3 定理 4 即知 $\zeta_k(s,\mathfrak{M},B)$ 可解析开拓至 $\mathrm{Re}(s)>1-\frac{1}{n_0}$，只在 $s=1$ 有单极点，留数为 $\rho_{\mathfrak{M}}$. 现令

$$\zeta_k(s,\mathfrak{M})=\sum_{B\in I(\mathfrak{M})/P_{\mathfrak{M}}}\zeta_k(s,\mathfrak{M},B)$$

$$=\sum_{(I,\mathfrak{M})=1}\frac{1}{NI^s}=\prod_{\wp\nmid\mathfrak{M}}(1-N\wp^{-s})^{-1}.$$

则 $\zeta_k(s,\mathfrak{M})$ 也在 $s=1$ 有单极点，留数为 $h_m\rho_m$，其余 $\mathrm{Re}(s)>1-\frac{1}{n_0}$ 各点均解析，显然 Dedekind Zeta 函数

$$\zeta_k(s)=\zeta_k(s,\mathfrak{M})\prod_{\wp\mid\mathfrak{M}}\frac{1}{1-N\wp^{-s}},$$

故知

$$h\rho=h_{\mathfrak{M}}\rho_{\mathfrak{M}}\prod_{\wp\mid\mathfrak{M}}(1-N\wp^{-1})^{-1}.$$

其中 $h=h_k$，$\rho=\rho_k$ 见 §8.4 和 §8.5，$h_{\mathfrak{M}}$ 见 §9.2.

域 k 的射线理想类群 $G(\mathfrak{M})=\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}$ 是有限 Abel 群，故有特征群$\widehat{G(\mathfrak{M})}$. 其中任一特征 χ 的定义可扩展到 k 的每个整理想 I(当 I 与 $\mathfrak{M}_0$ 不互素时令 $\chi(I)=0$). 定义 Hecke $L-$函数为

$$L_k(s,\chi)=\prod_{\wp}(1-\chi(\wp)/N\wp^s)^{-1}\quad(\mathrm{Re}(s)>1)$$

其中 $\wp$过 k 的素理想，考虑

$$-\sum_{\wp}(1-\chi(\wp)/N\wp^s)=\sum_{\wp,m}\frac{\chi(\wp)^m}{mN\wp^{ms}}=\sum_{\wp,m}\frac{\chi(\wp)^m}{mp^{f(\wp)ms}},$$

$$\sum_{\wp,m}\left|\frac{\chi(\wp)^m}{mp^{f(\wp)ms}}\right|=\sum_{\wp,m}\frac{1}{mp^{f(\wp)m\sigma}}\leqslant\sum_{\wp,m}\frac{1}{mp^{m\sigma}}\leqslant\sum_{p,m}\frac{n}{mp^{m\sigma}}$$
$$=n\log\zeta(\sigma).$$

故知当 $\mathrm{Re}(s)=\sigma>1$ 时，此级数绝对收敛，从而 $L_k(s,\chi)$收敛，故此时

$$\log L_k(s,\chi)=\sum_{\wp}\sum_{i}\frac{\chi(\wp)^i}{iN\wp^{is}}\sim\sum_{\wp}\frac{\chi(p)}{N\wp^s}$$

(对所有 $\wp$，或对使 $f(\wp)=1$ 的 $\wp$). 也有

$$L_k(s,\chi)=\sum_{I}\frac{\chi(I)}{NI^s}$$
$$=\sum_{B\in G(\mathfrak{M})}\sum_{I\in B}\frac{\chi(I)}{NI^s}$$
$$=\sum_{B\in G(\mathfrak{M})}\chi(B)\zeta_k(s,\mathfrak{M},B).$$

因此 $L_k(s,\chi)=\sum\limits_{i=1}^{\infty}\frac{b_i}{i^s}$ 的系数部分和 $A_i^L=b_1+\cdots,+b_i=\sum\limits_{B}\chi(B)\rho_{\mathfrak{M}}i+\sum\limits_{B}\chi(B)O(i^{1-1/n_0})$，这是利用了上述 $\zeta_k(s,\mathfrak{M},B)$

的估计，注意此处 $O(i^{1-1/n_0})$ 是依赖于 B 的. 当 $\chi\neq 1$ 时，由特征的正交性可知 $\sum\limits_{B}\chi(B)=0$（§8.4 定理 3 的证明），故

$$A_i^L=O(i^{1-1/n_0}).$$

定理 1 Dirichlet 级数 $L_k(s,\chi)=\sum\limits_{I}\chi(I)/NI^s(\chi\neq 1)$ 在复半平面 $\mathrm{Re}(s)>1-1/n_0$ 收敛，解析，是 Hecke L—函数 $L_k(s,\chi)$（原对 $\mathrm{Re}(s)>1$ 定义）的解析开拓.

证明 由上述对系数部分和 A_i^L 的估计，§8.3 定理 4（$\rho=0$ 情形）或定理 2，即得定理. □

如像 Dirichelet 特征一样，对每个 $\chi\in\widehat{G(\mathfrak{M})}$ 也可定义它的导子，从而定义本原特征. 当本原特征 $\chi=1$ 时，显然 $L_k(s,\chi)=\zeta_k(s)$.

定理 2（通用范指数不等式，第二不等式） 设 K/k 为 n 次 Galois 扩张，$\mathfrak{M}$ 是 k 的模，含所有分歧素除子，则 $h\leqslant n$，即

$$(\boldsymbol{I}(\mathfrak{M}):P_{\mathfrak{M}}\mathcal{N}(\mathfrak{M}))\leqslant[K:k].$$

证明 记 $H=\boldsymbol{P}_{\mathfrak{M}}\mathcal{N}(\mathfrak{M})$，$h=\#\boldsymbol{I}(\mathfrak{M})/H)$，$1\neq\chi\in(\boldsymbol{I}(m)/H)^\wedge$. 已知 HecKe L-函数 $L_k(s,\chi)$ 在 $\mathrm{Re}(s)>1-1/n_0$ 解析，现要证

$$L_k(1,\chi)\neq 0.$$

为此设

$$L_k(s,\chi)=(s-1)^{m(\chi)}g(s,\chi),\quad m(\chi)\geqslant 0, g(1,\chi)\neq 0.$$

则

$$\log L_k(s,\chi) \sim m(\chi)\log(s-1) \sim -m(\chi)\log\frac{1}{s-1}.$$

但由定义可知

$$\log L_k(s,\chi) \sim \sum_{\wp}\frac{\chi(\wp)}{N\wp^s} = \sum_{B\in I(\mathfrak{M})/H}\chi(B)\sum_{\wp\in B}\frac{1}{N\wp^s}.$$

对 $\chi\in(I(\mathfrak{M})/H)^\wedge$ 相加：

$$\sum_{\chi}\log L_k(s,\chi) \sim \sum_{\chi}\sum_{B}\chi(B)\sum_{\wp}\frac{1}{N\wp s}$$
$$= \sum_{B}\sum_{\wp}\frac{1}{N\wp^s}\sum_{\chi}\chi(B) = h\sum_{\wp\in H}\frac{1}{N\wp^s},$$

而

$$\sum_{\chi}\log L_k(s,\chi) = \log\zeta_k(s) + \sum_{\chi\neq 1}\log L_k(s,\chi)$$
$$\sim \log\frac{1}{s-1} + \sum_{\chi\neq 1}(-m(\chi))\log\frac{1}{s-1}.$$

令 $s\to 1^+$，则有

$$(1-\sum_{\chi\neq 1}m(\chi))\log\frac{1}{s-1} \sim h\sum_{\wp\in H}\frac{1}{N\wp s}$$
$$\gtrsim h\sum_{\wp\in S_{K/k}}\frac{1}{N\wp^s} \gtrsim \frac{h}{n}\sum_{f(\mathfrak{B})=1}\frac{1}{N\mathfrak{B}^s}$$
$$\gtrsim \frac{h}{n}\log\frac{1}{s-1}.$$

其中 $f\gtrsim g$ 意义为 $f\geqslant g+c$（c 为在 $s=1$ 的解析函数），$S_{K/k}$ 为 k 的（在 K）完全分裂的素理想集，$f(\mathfrak{B})=f(\mathfrak{B}|\wp)$. 注意对完全分裂的 $\wp$，其因子 $\mathfrak{B}$ 的范 $N(\mathfrak{B})=\wp$，故 $S_{K/k}\subset H=P_{\mathfrak{M}}\mathcal{N}(\mathfrak{M})$. 所以

$$1-\sum_{\chi\neq 1}\mathfrak{M}(\chi)\geqslant h/n>0.$$

故知 $m(\chi)=0$,即 $L_k(1,\chi)\neq 0$. 从而 $1\geqslant h/n$, $h\leqslant n$. 证毕.

系 1 设 K/k 为 n 次 Galois 扩张,则

$$(\boldsymbol{J}_K : k^{\cdot}N\boldsymbol{J}_K)\leqslant n,\quad (C_k : NC_K)\leqslant n.$$

§9.5 上同调理论

以下要为证明第一不等式 $h\geqslant n$ 作准备,一般都需要群的上同调理论. 我们事实上只用到 Herbrand 商. 但为了交待背景和阅读文献方便,下面先介绍上同调的基本理论. 再证明 Herbrand 商的性质. 读者也可以跳过上半节,直接从定理 2 前阅读.

设 G 是群,$R=\mathbf{Z}[G]$为群环(即 G 中元素形式上的整系数线性组合全体). 一个 R-模 M 也称为 G-模. 令

$$P_i=\mathbf{Z}[G^{i+1}]=\mathbf{Z}[g_0,g_1,\cdots,g_i)\,|\,g_i\in G],$$

即是由$(g_0,\cdots,g_i)$全体在 $\mathbf{Z}$ 上生成的自由 Abel 群(亦即 P_i 的元素为 诸$(g_0,\cdots,g_i)$的整数系数线性组合). P_i 按如下运算为 G-模:$s(g_0,\cdots,g_i)=(sg_0,\cdots,sg_i)$(对 $s\in G$). 于是 P_i 的 G-生成元系可取为$\{(1,g_1,\cdots,g_i)\}$或$\{(1,g_1,g_1g_2,g_1g_2g_3\cdots,g_1g_2\cdots g_i)\}$. 设 $d=d_i$ 为 G-模同态 $d:P_i\to P_{i-1}$,定义为

$$d(g_0,\cdots,g_i)=\sum_{j=0}^{i}(-1)^j(g_0,\cdots,g_{j-1},g_{j+1},\cdots,g_i),$$

令

$$\varepsilon(g_0)=1,$$

注意 $d_id_{i+1}=0$, $\varepsilon d_1=0$. 作长正合序列

$$P:\ \cdots P_i \xrightarrow{d_i} P_{i-1} \to \cdots \to P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} \mathbf{Z} \to 0$$

(这也称为 $\mathbf{Z}$ 的自由完全表现). 上述序列正合的意思是像 $\mathrm{Im} d_i = \mathrm{Ker} d_{i-1} (\forall\ i)$, $\mathrm{Im} d_1 = \mathrm{Ker}\varepsilon$, ε 为满射.

对任一 G-模 A, 令

$$K^i = \mathrm{Hom}_G(P_i, A)$$

为 P_i 到 A 的 G-模同态全体. 则由 P 得到

$$K:\ \cdots K^i \xleftarrow{d^{i-1}} K^{i-1} \leftarrow \cdots \leftarrow K^2 \leftarrow K^1 \leftarrow K^0 \xleftarrow{\varepsilon} K^{-1} \leftarrow 0.$$

其中 $d^{i-1}(\varphi) = \varphi d_i$. 因 $\varphi \in K^i$ 由其在 P_i 的生成元系 $\{(1, g_1, g_1 g_2, \cdots, g_1 \cdots g_i)\} = \{[g_1, \cdots, g_i]\}$ 上的值唯一决定, 故每个 φ 对应且仅对应一个 G^i 到 A 的映射

$$\varphi:\ [g_1, \cdots, g_i] \longmapsto \varphi(1, g_1, g_1 g_2, \cdots, g_1 \cdots g_i),$$

亦即 $\quad K^i = \mathrm{Hom}_G(P_i, A) = \{\text{映射 } \varphi:\ G^i \to A\}.$

群 G 对 A 的上同调群定义为

$$\widehat{H}^q(G, A) = \mathrm{Ker}\ d^q / \mathrm{Im}\ d^{q-1} \quad (q = 0, 1, \cdots).$$

注意 $\widehat{H}^q(G, A)$ 的元素不外乎是集合间某些映射 $\varphi:\ G^q \longrightarrow A$ 的同余类.

d^q 的作用可具体求出如下:

$$(\varepsilon\varphi)(g_0) = \varphi(\varepsilon g_0) = \varphi(1) = 0.$$

$$(d^0\varphi)[g_1] = \varphi d(1, g_1) = \varphi(g_1(1) - (1)) = g_1\varphi(1) - \varphi(1),$$

$$\begin{aligned}(d^1\varphi)[g_1, g_2] &= \varphi d(1, g_1, g_1 g_2) \\ &= \varphi(g_1(1, g_2) - (1, g_1 g_2) + (1, g_1)) \\ &= g_1\varphi[g_2] - \varphi[g_1 g_2] + \varphi[g_1],\end{aligned}$$

$$\begin{aligned}(d^2\varphi)[g_1, g_2, g_3] &= \varphi d(1, g_1, g_1 g_2, g_1 g_2 g_3) \\ &= \varphi(g_1(1, g_2, g_2 g_3) - (1, g_1 g_2, g_1 g_2 g_3) \\ &\quad + (1, g_1, g_1 g_2 g_3) - (1, g_1, g_1 g_2))\end{aligned}$$

$$=g_1\varphi[g_2,g_3]-\varphi[g_1g_2,g_3]$$
$$+\varphi[g_1,g_2g_3]-\varphi[g_1,g_2].$$

由此可知

$\widetilde{H}^0(G,A)=A^G$　　(A 的 G-不变元集),

$$\widetilde{H}^1(G,A)=\frac{\{\varphi: G\to A\mid\varphi(g_1g_2)=\varphi(g_1)+g_1\varphi(g_2)\}}{\{\varphi: G\to A\mid\varphi(g)=ga-a,a\in A\}}=\frac{\text{交叉同态群}}{\text{主交叉同态子群}},$$

$\widetilde{H}^2(G,A)=$

$$\frac{\{\varphi: G^2\to A\mid g_1\varphi(g_2,g_3)-\varphi(g_1g_2,g_3)+\varphi(g_1,g_2g_3)-\varphi(g_1,g_2)=0\}}{\{\varphi: G^2\to A\mid\varphi(g_1,g_2)=g_1\varphi(g_2)-\varphi(g_1g_2)+\varphi(g_1)\}}.$$

注意,若映射 $\varphi: G\to A$ 满足 $\varphi(g_1g_2)=\varphi(g_1)+g_1\varphi(g_2)$,则称 φ 为交叉同态映射(试比较:满足 $\varphi(g_1g_2)=\varphi(g_1)+\varphi(g_2)$的称为同态),而其中满足 $\varphi(g)=ga-a$ ($a\in A$)的称为主交叉同态映射. $\widetilde{H}^1(G,A)$就是 G 到 A 的交叉同态集对主交叉同态集的商群. 同样,$\widetilde{H}^2(G,A)$是 G^2 到 A 的某种映射集的商群.

定理 1　对 G-模的任一短正合序列 $0\to B\to A\to C\to 0$,自然地有上同调群的长正合序列

$$0\to\widetilde{H}^0(G,B)\to\widetilde{H}^0(G,A)\to\widetilde{H}^0(G,C)\xrightarrow{\delta}$$
$$\widetilde{H}^1(G,B)\to\widetilde{H}^1(G,A)\to\widetilde{H}^1(G,C)\xrightarrow{\delta}$$
$$\widetilde{H}^2(G,B)\to\widetilde{H}^2(G,A)\to\widetilde{H}^2(G,C)\xrightarrow{\delta}\cdots\cdots$$

这里"自然"的意思是,短正合序列的平移将导制长正合序列平移后的交换图.

另一方面,令张量积

$$K_i = P_i \otimes_G A,$$

则由序列 P 可得长正合序列

$$K_* \quad \cdots \to K_{i+1} \xrightarrow{d_{i+1}} K_i \xrightarrow{d_i} K_{i-1} \to \cdots \to K_0 \to K_{-1} \to 0.$$

群 G 对 A 的同调群定义为

$$\widetilde{H}_q(G,A) = \mathrm{Ker}\ d_q / \mathrm{Im}\ d_{q+1} \quad (q=0,1,\cdots).$$

同调群也有类似于定理 1 的上同调群的性质，且

$$\widetilde{H}_0(G,A) = A_G = A/I_G A,$$

$$\widetilde{H}_1(G,A) = G/G',$$

其中 I_G 是 $\{s-1\}(s \in G)$ 生成的 $\mathbf{Z}[G]$ 的理想，G' 是 G 的换位子群.

对有限群 G,G-模 A 有如下的(取范或迹)自同态

$$\mathrm{tr}: A \to A, \qquad a \longmapsto \sum_{s \in G} s(a).$$

显然 $\mathrm{Ker}\ (\mathrm{tr}) \supset I_G A$, $\quad \mathrm{Im\ tr} \subset A^G$. 令

$$H^0(G,A) = A^G / \mathrm{tr} A,$$

$$H^{-1}(G,A) = A_{t_r} / I_G A \quad (A_{t_r} 是 t_r 在 A 的核)$$

$$H^q(G,A) = \begin{cases} \widetilde{H}^q(G,A), & 当\ q > 0. \\ \widetilde{H}_{|q|-1}(G,A), & 当\ q < -1. \end{cases}$$

$H^q(G,A)$称为 **Tate 上同调群**(它们也可由连结长序列 K 和 K_* 而定义，也有类似定理 1 的性质).

特别，当 $G = \langle \sigma \rangle$ 是 n 阶循环群时，可以从定义 H^q 的长序列中抽出一个子序列，使得 $H^q(G,A)$ 由下列序列定义：

$$\cdots A \xrightarrow{1-\sigma} A \xrightarrow{t_r} A \xrightarrow{1-\sigma} A \xrightarrow{t_r} A \to \cdots$$

(注意有 $\mathrm{tr}(1-\sigma) = (1-\sigma)\mathrm{tr} = 0$). 故对 $q \in \mathbf{Z}$ 有

$$H^{2q}(G,A) = H^0(G,A) = \mathrm{Ker}(1-\sigma)/\mathrm{Im}\ t_r = A^G/\mathrm{tr}A,$$

$$H^{2q+1}(G,A)=H^{-1}(G,A)=\mathrm{Ker}\ \mathrm{tr}/\mathrm{Im}(1-\sigma)=A_{\mathrm{tr}}/I_G A.$$

且对任一短正合序列 $0\to B\xrightarrow{i}A\xrightarrow{j}C\to 0$,对应的长正合序列化为"六边形":

$$\begin{array}{ccccc} & H^0(G,A) & \xrightarrow{j} & H^0(G,C) & \\ {}^{i}\nearrow & & & & \searrow^{\delta_1} \\ H^0(G,B) & & & & H^{-1}(G,B) \\ {}_{\delta_2}\nwarrow & & & & \swarrow_{i} \\ & H^{-1}(G,C) & \xleftarrow{j} & H^{-1}(G,A) & \end{array}$$

Herbrand 商定义为

$$Q(G,A)=\frac{\# H^0(G,A)}{\# H^{-1}(G,A)}=\frac{(A^G:\mathrm{tr}A)}{(A_{\mathrm{tr}}:I_G A)}.$$

例如,$\mathbf{Z}$ 是平凡 G-模($g(i)=i$),当 G 为循环群时,$H^0(G,\mathbf{Z})=\mathbf{Z}^G/\mathrm{tr}\mathbf{Z}=\mathbf{Z}/|G|\mathbf{Z}$, $H^{-1}(G,\mathbf{Z})=\mathbf{Z}_{\mathrm{tr}}/I_G\mathbf{Z}=0/I_G\mathbf{Z}=0$,$Q(G,\mathbf{Z})=$
$|G|=\# G$.

再如,若 K/k 为 Galois 扩张,$G=G(K/k)$,则 K^* 是 G-模. $K^{*G}=k^*$,$\mathrm{tr}K^*=N_{K/k}K^*$. 故 $H^0(G,K^*)=K^{*G}/\mathrm{tr}K^*=k^*/NK^*$. 其元素个数也是一种范指数.

上述定义可稍作推广. 设 A 为 Abel 群,f 和 g 是 A 的自同态且 $fg=gf=0$. 则有正合列

$$\cdots\to A\xrightarrow{f}A\xrightarrow{g}A\xrightarrow{f}A\xrightarrow{g}\cdots$$

令

$$H^0(A)=\mathrm{Ker}f/\mathrm{Im}g,\qquad H^{-1}(A)=\mathrm{Ker}g/\mathrm{Im}f,$$

定义 A 对 f,g 的 **Herbrand 商**为

$$Q(A)=\frac{\# H^0(A)}{\# H^{-1}(A)}=\frac{(\mathrm{Ker}f:\mathrm{Im}g)}{(\mathrm{Ker}g:\mathrm{Im}f)}.$$

特别若 $G=<\sigma>$ 是 n 阶循环群，A 为 G-模，令

$$f=1-\sigma,\quad g=1+\sigma+\cdots+\sigma^{n-1}=\mathrm{tr}$$

则可知 $fg=gf=0$，且

$$H^0(A)=\mathrm{Ker}f/\mathrm{Im}g=A^G/\mathrm{tr}A=H^0(G,A),$$

$$H^{-1}(A)=\mathrm{Ker}g/\mathrm{Im}f=A_{\mathrm{tr}}/(1-\sigma)A=H^{-1}(G,A),$$

$Q(A)=Q(G,A)$，与上述一致.

引理 1(三指数引理) 设 f 是 Abel 群 A 到某群的同态，以 A^f，A_f 记 f 的象与核. 若 B 是 A 的子群，则

$$(A:B)=(A^f:B^f)(A_f:B_f)$$

(若三指数中有二个有限，则均有限且此等式成立).

证明 考虑 $A\to A^f\to A^f/B^f$，在 A 的核为 $B+A_f$，故 $A/(B+A_f)\cong A^f/B^f$. 又因 $A\supset B+A_f\supset B$，且 $(B+A_f)/B\cong A_f/(A_f\cap B)=A_f/B_f$，即得引理. □

定理 2 设 $0\longrightarrow B\xrightarrow{i}A\xrightarrow{j}C\longrightarrow 0$ 为 Abel 群的正合列，f，g 为 A 的同态且 B(作为 A 的子群)在 f，g 作用下封闭，且 $fg=gf$. 于是 f，g 也是 $C(\cong A/B)$的同态. 则 Herbrand 商满足(积性)：

$$Q(A)=Q(B)Q(C)$$

且当 A 为有限群时

$$Q(A)=1.$$

证明 记 f 在 A 的核为 A_f，象为 A^f. 当 $(A:B)$ 有限时，由

"三指数引理"

$$(A:B)=(A^f:B^f)(A_f:B_f),$$

右方等于

$$(A^f:B^f)(A^g:B^g)\frac{(A_f:A^g)}{(B_f:B^g)},$$

最后一个因子应对 f,g 对称,即知 $(A_f:A^g)/(B_f:B^g)=(A_g:A^f)/(B_g:B^f)$,即得所欲证.

对一般情形,我们可得到上同调群构成的六边形:$H^0(B)\xrightarrow{i}H^0(A)\xrightarrow{j}H^0(C)\xrightarrow{\delta_1}H^{-1}(B)\xrightarrow{i}H^{-1}(A)\xrightarrow{j}H^{-1}(C)\xrightarrow{\delta_2}H^0(B)$(即前述六边形但不带标记 G),其中 i,j 分别由 $i: B\to A$, $j: A\to C$ 诱导,δ_1 定义如下:

$$\begin{array}{ccccccc}
* & \xrightarrow{i} & a & \xrightarrow{j} & c & \longrightarrow & 0 \\
\downarrow f & & \downarrow f & & \downarrow f & & \\
fa & \longrightarrow & fa & \xrightarrow{j} & 0 & \longrightarrow & 0 \\
\downarrow g & & \downarrow g & & \downarrow g & &
\end{array}$$

对 $c\in C_f$,取 A 中 $a\in j^{-1}(c)$,令 $\delta_1(c)=fa(\mathrm{mod}B^f)$(由 $c\in C_f$ 知 $fc=0$,故 $j(fa)=f(ja)=fc=0$, $fa\in B$. 从而 $g(fa)=(gf)a=0a=0$,知 $fa\in B_g$). 类似定义 δ_2,易验证上述六边形是正合序列.

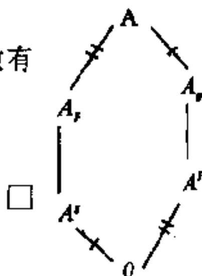
将上述六边形正合序列从任一项起依次记为 $M_1\xrightarrow{\varphi_1}M_2\to\cdots\xrightarrow{\varphi_5}M_6\xrightarrow{\varphi_6}M_1$. 记 $k_i=\#\mathrm{Ker}\varphi_i$, $m_i=\#\mathrm{Im}\varphi_{i-1}$. 则由正合性知 $k_i=m_i$,且因 $\mathrm{Im}\varphi_i\cong M_i/\mathrm{Ker}\varphi_i$(注意 $0\to\mathrm{Ker}\varphi_i\to M_i\to\mathrm{Im}\varphi_i\to 0$ 是正合序列),故 $|M|=\#M_i=m_{i+1}k_i$,从而

$$\mathfrak{M}_1\mathfrak{M}_3\mathfrak{M}_5k_2k_4k_6=k_1k_3k_5\mathfrak{M}_2\mathfrak{M}_4\mathfrak{M}_6,$$

$$|m_2||m_4||m_6|=|m_1||m_3||m_5|,$$

$$Q(A)=Q(B)Q(C).$$

若$|A|$有限，则因 $0\to A_f\to A\to A^f\to 0$ 正合，故有如下子群格，及同构 $A^f\cong A/A_f, A^g\cong A/A_g$，故



$$Q(A)=\frac{(A_f : A^g)}{(A_g : A^f)}=1.$$

□

§9.6 范指数

本节讨论局部域和整体循环域的范指数，先讨论一个一般性结果.

记G是有限群，G-模 $A=\coprod_{i=1}^{s} A_i$ 是诸 A_i 的直和，且G可迁地置换诸 A_i. 记 G_1 为 A_1 的固定子群($G_1=\{g\in G|gA_1=A_1\}$，也称 A_1 的分解群). 于是有陪集分解

$$G=\bigcup_{i=1}^{s}\sigma_i G_1,\quad A_i=\sigma_i A_1\quad(\sigma_1=1),$$

且A中元素均可表为 $a=a_1+\sigma_2 a_2+\cdots+\sigma_s a_s$，$a_j\in A_1$.(例如 $A=\coprod_{w|v} K_w^*$ 是 J_K 的 v-分量；再如 $A=K=Qw_1+\cdots+Qw_n$ 为数域K的整数环).

定理 1 设G，$A=\coprod A_i$ 如上，则有同构：

(1) $H^0(G,A)\cong H^0(G_1,A_1)$，由同构映射

$$\pi:\ A^G\to A_1^{G_1},\qquad a_1+\sigma_2 a_1+\cdots+\sigma_s a_1\longmapsto a_1$$

诱导($a_1\in A_1^{G_1}$).

(2) $H^{-1}(G,A)\cong H^{-1}(G_1,A_1)$，此同构由映射

λ: $A_{t_r} \to A_1 t_{r1}$, $\quad a_1+\sigma_2 a_2+\cdots+\sigma_s a_s \longmapsto a_1+\cdots+a_s$ 诱导($a_j \in A_1$, t_r 和 t_{r1} 为 G 和 G_1 的范(迹)).

证明 (1) 注意 $H^0(G,A)=A^G/t_rA$,而 $A^G=\{\sigma_1+\sigma_2 a_1+\cdots+\sigma_s a_1 \mid a_1\in A_1^{G_1}\}$. 事实上,若 $a=\sum \sigma_i a_i'$ 在 G 下固定,则对任一固定指标 j 以 σ_j^{-1} 作用,便得到 $a_j'=\sigma_j^{-1}\sigma_j a_j'$ 是 $\sigma_j^{-1}a=a$ 的 A_1-分量,故 $a_j'=a_1'(\forall j)$,故断言成立. 特别可知,A^G 中元素由其第一分量决定,故有同构

$$\pi:\quad A^G \longrightarrow A_1^{G_1}$$
$$a_1+\cdots+\sigma_s a_1 \longmapsto a_1.$$

而 $t_r(\sigma_j a_1)=\sum\limits_{\sigma\in G}\sigma\sigma_j a_1=\sum\limits_{\sigma}\sigma a_1=\sum\limits_{i=1}^{s}\sum\limits_{\sigma\in G_1}\sigma_i\sigma a_1=\sum\limits_{i=1}^{s}\sigma_i t_{r1}(a_1)$ $(a_1\in A_1)$,故

$$H^0(G,A)=A^G/t_rA=\frac{\pi(A^G)}{\pi(t_rA)}=\frac{A_1^{G_1}}{t_{r1}A_1}=H^0(G_1,A_1).$$

(2) 注意 $H^{-1}(G,A)=A_{t_r}/I_GA$. A 中任一元素可表为 $a=a_1+\sigma_2 a_2+\cdots+\sigma_s a_s$, $a_j\in A_1$. $a\in A_{t_r}\Leftrightarrow a_1+\cdots+a_s\in A_1 t_{r1}$,故 $\lambda: A_{t_r}\longrightarrow A_{1t_{r1}}$ 是满射. 再证 λ 映 I_GA 到 $I_{G_1}A_1$ 中:若 $\sigma\in G$,则存在指标 i 的置换 π 使 $\sigma\sigma_i=\sigma_{\pi(i)}\tau_{\pi(i)}$,某 $\tau_{\pi(i)}\in G_1$;故 $\lambda(\sigma a-a)=\sum\limits_{i=1}^{s}(\tau_{\pi(i)}a_i-a_i)$,断言得证. 只需再证若 $\lambda(a)=0$ 则 $a\in I_GA$. 事实上若 $a_1+\cdots+a_s=0$,则 $a=\sum\limits_{i=1}^{s}(\sigma_i a_i-a_i)\in I_GA$. 证毕. □

系 1 设 K/k 是 n 次 Galois 扩张,$G=G(K/k)$,则
$$H^0(G,K^+)=H^{-1}(G,K^+)=0.$$

而若 K/k 是循环扩张，则

$$H^{-1}(G,K^*)=1.$$

(K^+和 K^*为 K 的加法群和非 0 元乘法群，这是 Galois 上同调论的特例，事实上对有限扩张 K/k 和任意 q 总有 $H^q(G,K^+)=0, H^1(G,K^*)=1$).

证明 K/k 总有正规基，即存在 $w\in K$ 使 $\{\sigma w\mid\sigma\in G\}$是 K/k 的基：

$$K=kw\oplus k\sigma_2 w\oplus\cdots\oplus k\sigma_n w$$

显然 G 可迁地作用于诸分量，而分量个数等于 $n=|G|$，故 $G_1=\{1\}$，即知 $H^0(G,K^+)=H^0(1,kw)=0$， $H^{-1}(G,K^+)=H^{-1}(1,kw)=0$.

由 Hilbert 定理 90，当 K/k 为循环扩张时，对 $\beta\in K$ 有 $N_{K/k}\beta=1\Leftrightarrow\beta=\sigma\alpha/\alpha$(某 $\alpha\in K,\sigma\in G$)而 $K^*_{t_r}=\{\beta\in K^*\mid N\beta=1\}$，$I_G K^*=\{\beta=\sigma\alpha/\alpha\mid\alpha\in K^*\}(G=\langle\sigma\rangle)$. 故

$$H^{-1}(G,K^*)=K^*_{t_r}/\langle 1-\sigma\rangle K^*=1. \qquad \square$$

定理 2 设 K_w/k_v 是局部域的 n_v 次循环扩张(k_v 是 k 对 $\wp$-adic 赋值 $v=v_\wp$的完备化)，设 $G_v=\langle\sigma\rangle$是其 Galois 群，U_v,U_w 为 k_v 和 K_w 的单位群，$e=e(w|v)$为分歧指数，则

(1)(局部范指数)

$$\# H^0(G_v,K_w^*)=Q(G_v,K_w^*)=(k_v^*:N_w K_w^*)=n_v.$$

(2)(单位范指数)

$$\# H^0(G_v,U_w)=(U_v:N_w U_w)=e, \text{ 且 } \quad Q(G_v,U_w)=1.$$

证明 $(\# k_v^*/N_w K_w^*)/1=\# H^0(G_v,K_w^*)/\# H^{-1}(G_v,K_w^*)=Q(G_v,K_w^*)=Q(G_v,U_w)Q(G_v,\mathbf{Z})$，最后等号是因 $K_w^*=U_w\pi^{\mathbf{Z}}$

(π 是素元). 因 $\sigma\pi=u\pi$,故 G_v 平凡地作用于 $\mathbf{Z}$,即 $Q(G_v,\mathbf{Z})=n_v$.

设$\{w_\tau|\tau\in G_v\}$ 是 K_w/k_v 的正规基,乘以 k_v 的素元的适当幂,可设 w_τ 均是赋值非常小的整数. 于是 $K_w=\sum_\tau k_v w_\tau$. 令

$$M=\sum_{\tau\in G_v}O_v w_\tau,\qquad T=\prod_{\tau\in G_v}\exp(O_v w_\tau).$$

(其中 O_v 是 k_v 的整数环,$\exp(x)=1+x+\cdots+x^n/n!+\cdots$是 p-adic指数函数,对$|x|_v<p^{-1/(p-1)}$收敛,$(p)=\wp\cap\mathbf{Z}$ 见 § 8.7).
故有如下等式(理由在下面解释):

$$1\overset{(1)}{=\!=}Q(G_1,O_v w_1)\overset{(2)}{=\!=}Q(G_v,M)\overset{(3)}{=\!=}Q(G_v,T)=$$
$$\overset{(4)}{=\!=}Q(G_v,U_w)/Q(G_v,U_w/T)\overset{(5)}{=\!=}Q(G_v,U_w),$$

其中(1)是因为 $G_1=\{1\}$(G_1 是 $O_v w_1$ 的不变子群,因 w_τ 是正规基故 $G_1=\{1\}$);(2)因上节定理 1;(3)因 $M\cong T$(exp 与 log 互为逆);(4)因 Q 的积性;(5)因 $Q(G_v,U_w/T)=1$,这是由于 U_w/T 为有限群(M 是含 0 开集,故 T 是含 1 开子群,故 $T=1+\mathfrak{P}^r$).

(2)$Q(G_v,U_w)=\#H^0(G_v,U_W)/\#H^{-1}(G_v,U_w)=(U_k:N_wU_w)/(H:U_w^{1-\sigma})$,其中,$H$ 为范映射在 U_w 中核$\subset$范在 K_w^* 中核$=K_w^{*(1-\sigma)}\subset$范在 U_w 中核(等号是由 Hibert 定理 90,最后"属于号"是因 $\alpha^{1-\sigma}$均为单位). 故得到 $H=K_w^{*(1-\sigma)}$. 从而

$$(H:U_w^{1-\sigma})\overset{(1)}{=\!=}(K_w^{*(1-\sigma)}:(k_v^*U_w)^{1-\sigma})$$
$$\overset{(2)}{=\!=}\frac{(K_w^*:k_v^*U_w)}{((K_w^*)_{1-\sigma}:(k_v^*U_w)_{1-\sigma})}\overset{(3)}{=\!=}\frac{e}{(k_v^*:k_v^*)}=e.$$

其中(1)是由$(k_v^*)^{1-\sigma}=1$;(2)由三指数引理;(3)由 $K_w^*=U_w\pi_w^{\mathbf{Z}}$,$k_v^*=U_v\pi^{\mathbf{Z}}=U_v\pi_w^{e\mathbf{Z}}$,得分子为 e;再因$(K_w^*)_{1-\sigma}$即是 K_w^* 中 σ—不变

元，故为 k_v^*.

系 2(1) 若 K_w/k_v 不分歧(即 $e=1$)，则 $U_v=N_wU_w$.

(2) 对 n_v 次 Abel 局部扩域 K_w/k_v，总有

$$(k_v^*:N_wK_w^*)\leqslant n_v.$$

$$(U_v:N_wU_w)\leqslant e.$$

证明 (1)显然. (2)K_w/k_v 可通过有限次循环扩张得到，而对于 $K\supset E\supset k$ 有

$$(k^*:N_{K/k}K^*)=(k^*:N_{E/k}E^*)(N_{E/k}E^*:N_{E/k}N_{K/E}K^*)$$
$$\leqslant(k^*:N_{E/k}E^*)(E^*:N_{K/E}K^*).$$ □

定理 2 对 $k_v=\boldsymbol{R}$ 和 $\boldsymbol{C}$ 也是成立的.

9.6.1 整体循环范指数

设 K/k 为数域的 Galois 扩张，$G=G(K/k)$；S 是 k 的素除子子集，含所有无限素除子；S_K 是 S 中元素在 K 的延拓集，对任一 $w\in S_K$，取一个符号 X_w，以 E^S 记$\{X_w\}(w\in S_K)$在 $\boldsymbol{R}$ 上生成的 $s=\#S$ 维向量空间. 对 $\sigma\in G$ 定义 $\sigma X_w=X_{\sigma w}$，并线性地扩展为 G 对 E^S 的作用.

定理 3(Artin－Tate) E^S 中的任一个 G-不变格 M 均有 G-不变子格 M' 使 M' 有 $\boldsymbol{Z}$-基$\{Y_w\}(w\in S_K)$满足 $\sigma Y_w=Y_{\sigma w}(\sigma\in G)$，且 M' 在 M 中指数有限. (E^s 中的格是指其子群 M，M 的 $\boldsymbol{Z}$-基也是 E^S 的 $\boldsymbol{R}$-基. M 为 G-不变是指对 $\sigma\in G$ 均有 $\sigma M\subset M$).

证明 对 E^S 在$\{X_w\}$下的坐标系取 E^S 的 sup- 范(即向量

的范取为其坐标赋值的sup). 因 M 是格，故存在数 b 使对任一 $X \in E^s$ 有某 $Z \in M$ 满足 $|X - Z| < b$. 对 $v \in S$ 设 $\bar{v} \in S_K$ 使 $\bar{v}|v$. 取大正数 t 及某 $Z_{\bar{v}} \in M$ 使 $|tX_{\bar{v}} - Z_{\bar{v}}| < b$. 对 $w|v$ 令 $Y_w = \sum_{\sigma\bar{v}=w} \sigma Z_{\bar{v}}$（求和是对所有使 $\sigma\bar{v} = w$ 的 $\sigma \in G$). 断言 $\{Y_w\}$ 满足定理.

首先对 $\tau \in G$ 有 $\tau Y_w = \sum_{\sigma\bar{v}=w} \tau\sigma Z_v = \sum_{\rho\bar{v}=\tau w} \rho Z_{\bar{v}} = Y_{\tau w}$. 其中第 2 和式对满足 $\rho\bar{v} = \tau w$ 的所有 $\rho \in G$ 求和，作变换 $\rho = \tau\sigma$. 再证 $\{Y_w\}$ 在 $\boldsymbol{R}$ 上线性无关. 设 $\sum c_w Y_w = 0$（$c_w \in \boldsymbol{R}$ 不全为 0)，可设 $|c_w| \leqslant 1$（$\forall\ w$) 且对某 w_0. 有 $|c_{w_0}| = 1$. 记 $Z_{\bar{v}} = tX_{\bar{v}} - B_{\bar{v}}$，向量 $B_{\bar{v}}$ 满足 $|B_{\bar{v}}| < b$. 则 $Y_w = \sum_{\sigma\bar{v}=w} \sigma Z_{\bar{v}} = t\sum_{\sigma\bar{v}=w} X_{\sigma\bar{v}} + B'_w$, $|B'_w| \leqslant nb$, $n = \#G$. 故 $Y_w = tm_w X_w + B'_w$, mM_w 是使 $\sigma\bar{v} = w$ 的 $\sigma \in G$ 个数. 从而 $0 = \sum_w c_w Y_w = t\sum_w c_w m_w X_w + B'$, $|B'| \leqslant snb$. 注意 w_0 使 $|c_{w_0}| = 1$ 一项，当 t 适当大时则矛盾. □

注意 M' 是 G-同构于以 $\{X_w\}$ 为基的格，可分解为直和

$$M' = \prod_{v\in S} \prod_{w|v} \mathbf{Z}Y_W.$$

每个子群 $M'_v = \prod_{w|v} \mathbf{Z}Y_w$ 是半局部的（即 G 可迁地置换诸 $\mathbf{Z}Y_w$)，每个有分解（固定）群 G_w（在 $\mathbf{Z}Y_w$ 上作用平凡，而 $\mathbf{Z}Y_w$ 是 G_w－同构于 $\mathbf{Z}$ 的).

系 3 设 $G=G(K/k)$ 为 n 阶循环群，则

(1) $Q(G,M) = Q(G,M') = \prod_{v\in S} n_v$

(其中 $n_v=[K_w:k_v]$, $w|v$).

(2) $Q(G,K_S) = \frac{1}{n}\prod_{v\in S} n_v$

(其中 K_S 为 K 的 S-单位群,见§9.1).

证明 (1) 记 $M'_v = \prod_{w|v}(\mathbf{Z}Y_w)$,则 $M' = \prod_{v\in S} M'_v$,且 M'_v 满足上节所设:G 可迁地作用于其分量. $\mathbf{Z}Y_w$ 的固定群即是 w 的分解群 G_w(因 $\sigma w = w$). 故由 $(M:M')$ 有限知 $Q(G,M) = Q(G,M') = \prod_{v\in S} Q(G,M'_v) = \prod_{v\in S} Q(G_{w_1},\mathbf{Z}Y_{w_1}) = \prod_{v\in S} n_v$,最后等号是因 G_{w_1} 平凡作用于 $\mathbf{Z}Y_{w_1}\cong\mathbf{Z}$.

(2) $K_S \longrightarrow E^S$, $u\longrightarrow \sum_{w\in S_K}\log\|u\|_w X_w$ 是 G- 模同态,记为 l. 则 l 的象为 E^S 中 s-1 维超平面的格,核(即单位根)有限. 令 E^S 中向量 $X_0 = \sum_{w\in S_K} X_w$, $M = l(K_S)\oplus\mathbf{Z}X_0$(是 X_0 与 $l(K_S)$ 生成的格),由(1) 知 $Q(G,K_S) = Q(G,l(K_S)) = Q(G,M)/Q(G,\mathbf{Z}X_0) = (\prod nu)/n$. □

定理 4 设 K/k 为数域的 n 次循环扩张,$G = G(K/k)$,则 $H^{-1}(G,C_K) = 1$ 且类群的范指数 $h = n$,即

$$(C_k:NC_K) = (\boldsymbol{J}_k:k^*N\boldsymbol{J}_K) = (\boldsymbol{I}(\mathfrak{M}):\boldsymbol{P}_{\mathfrak{M}}\mathcal{N}(\mathfrak{M})) = n.$$

证明 设 S 是 K 的素除子子集,含所有分歧和无限素除子,且使 $\boldsymbol{J}_K = K^*\boldsymbol{J}_{K,S}$(§9.1(12) 式). 也可设 S 在 G 作用下不

变. 于是 $Q(G,C_K)=Q(G,K^*J_{K,S}/K^*)=Q(G,J_{K,S}/K_S)=$
$$Q(G,J_{K,S})/Q(G,K_S).$$
$$J_{K,S}=\prod_{v\in S_k}(\prod_{w|v}K_w^*)\times\prod_{v\notin S_k}(\prod_{w|v}U_w)=V_1\times V_2$$
(S_k 是 S 在 k 限制). 故出上述局部范指数 $Q(G,\prod_{w|v}U_w)=Q(G_{w_1},U_{w_1})=1$ 知 $Q(G,\prod_{w|v}K_w^*)=Q(G_{w_1},K_{w_1}^*)=n_v$. 故 $Q(G,J_{K,S})=\prod_{v\in S_k}n_v$. $n=Q(G,C_K)=\#H^0(G,C_K)/\#H^{-1}(G,C_K)=(C_k:NC_K)/\#H^{-1}(G,C_K)\leqslant n/\#H^{-1}(G,C_K)$(由通用范指数不等式). □

系 4 设 K/k 为数域循环扩张($K\neq k$),则 k 中有无限多个素理想 $\wp$ 在 K 不完全分裂.

证明 设只有有限集 S 中的素理想 $\wp$ 不分裂. 若 $v\notin S$ 则 v 分裂,故 $k_v=K_w(\forall\ w|v)$. 故 $k_v^*=NK_w^*$. 对任一 $a=(a_v)\in J_k$,由逼近定理知存在 $\alpha\in k^*$ 使 $\alpha a_v\approx1(\forall\ v\in S)$. 因 NK_w^* 是 1 的一个开子集,必含 $\alpha a_v(v\in S)$. 故 $\alpha a\in NJ_K$, $a\in k^*NJ_K$, $J_k=k^*NJ_K$,从而 $n=1$ 矛盾.

注记 1 设 K/k 是循环扩张,由正合列 $0\longrightarrow K^*\xrightarrow{i}J_K\xrightarrow{j}C_K\longrightarrow0$,有正合列 $1=H^{-1}(G,C_K)\xrightarrow{\delta}H^0(G,K^*)\xrightarrow{i}H^0(G,J_K)$. 故 i 为单射. 由定义即得 Hasse 定理:若 K/k 为循环扩张,则 $\alpha\in k^*$ 是整体范 $\Leftrightarrow\alpha$ 处处为局部范. (对非循环扩张一般不成立). 再考虑上述长正合列另一段:$1=H^1(G,C_K)\xrightarrow{\delta}$

$H^2(G,K^*) \xrightarrow{i} H^2(G,J_K)$. 单射 i 的含义恰为 Albert-Hasse-Brauer-Noether 定理：一个单代数（或 2－闭链）整体分裂 ⇔ 它处处局部分裂.（这对任一 Galois 扩张 K/k 均成立，即有 $H^1(G,C_K)=1$，且由循环情形易推广至 Galois 扩张）（见[A-T]）.

§9.7 Artin 互反律

设 K/k 为 Abel 扩张，$G=G(K/k)$，k 的素理想 $\wp$ 在 K 不分歧，$q=N\wp=p^{f_0}=\#k$，$\mathfrak{P}|\wp$ 为 K 的素理想. 于是 $\overline{K}=\boldsymbol{F}_{q^f}$，$\overline{k}=\boldsymbol{F}_q$，$\overline{G}=G(\overline{K}/\overline{k})=\langle\overline{\sigma}\rangle$ 是 $f=f(\mathfrak{P}|\wp)$ 阶循环群. $\overline{\sigma}$ 在 $G_{\mathfrak{P}}\subset G$ 中的原象即为 Frobenius 自同构，记为

$$\sigma=\sigma_\wp=(\wp,K/k)=\left(\frac{K/k}{\wp}\right).$$

由下式唯一刻画：

$$(\wp,K/k)\alpha\equiv\alpha^{N\wp}(\mathrm{mod}\mathfrak{P})(\forall\ \alpha\in O_K).$$

于是 k 的每个非分歧素理想 $\wp$ 对应于一个 G 中元 $(\wp,K/k)$. 按积性将此对应扩展为理想群到 Galois 群映射

$$\begin{aligned}\mathscr{A}:\quad & I(\mathfrak{M})\longrightarrow G\\ & \wp\longmapsto(\wp,K/k)\end{aligned}$$

其中 $\mathfrak{M}$ 是 k 的任一模，含所有分歧的素除子. $\mathscr{A}=\mathscr{A}_m$ 称为 **Artin（互反律）映射**，$(\wp,K/k)$ 称为 **Artin（互反律）符号**. 我们曾在 §3.6 和本章开始提及.

注意 $\sigma_\wp$ 的作用实质上只与 $N\wp=\#k$ 有关：对任一代数数 $\alpha\in K$（某 K），$\sigma_\wp(\alpha)=\alpha^q(\mathrm{mod}\mathfrak{P})$，$\mathfrak{P}$ 为 $\wp$ 在 K 的素因子. 故若令 $\boldsymbol{A}$ 是 k 的最大 Abel 扩张，则可定义 Artin 符号 $(\wp,\boldsymbol{A}/k)$：它在 K 上的限制即为 $(\wp,K/k)$，记为

$$(\wp, A/k)_K = (\wp, K/k).$$

由 §3.6 知 Artin 符号有如下性质：

(*A*1)(域同构-群共轭) 设 $\tau: K \to \tau K$ 为域同构(不一定固定 k)，则

$$(\tau I, \tau K/\tau k) = \tau(I, K/k)\tau^{-1}.$$

(*A*2)(扩域下限制) 设 $L \supset K \supset k$ 均为 Abel 扩张，则

$$(I, L/k)_K = (I, K/k).$$

(*A*3)(基域下取范) 设 k'/k 为有限扩张，则

$$(I, A/k') = (N_{k'/k}I, A/k),$$

特别对 k' 的素理想 $\wp' \mid \wp$ 有

$$(\wp', A/k') = (N\wp', A/k) = (\wp, A/k)^{f(\wp'|\wp)}.$$

上述(*A*3)也可用有限扩张记法写为

$$(I, Kk'/k')_K = (N_{k'/k}I, K/k),$$

$$(\wp', Kk'/k')_K = (\wp, K/k)^{f(\wp'|\wp)};$$

特别当 $K \supset k' \supset k$ 时则 $(I, K/k') = (N_{k'/k}I, K/k)$.

特别应注意的是，$(\wp, K/k)$ 的阶为 $f(\mathfrak{P}|\wp)$. 因此 $(\wp, K/k) = 1 \Leftrightarrow f(\mathfrak{P}|\wp) = 1 \Leftrightarrow \wp$ 在 K 完全分裂.

定理 1 Artin 映射 $\mathscr{A}: I(\mathfrak{M}) \to G$ 是满射.

证明 设 $\mathrm{Im}\mathscr{A}$ 的固定子域为 $F \neq k$. 则对 $\wp \in I(\mathfrak{M})$ 有 $(\wp, F/k) = (\wp, K/k)_F = 1$，即 $\wp$ 在 F 完全分裂. 故在 F(从而在其循环子域 F_0) 不完全分裂的 $\wp$ 只有 $\wp \mid \mathfrak{M}_0$，这与上节最后定理矛盾. □

以下要确定核 $\mathrm{Ker}\mathscr{A} = \ker(-, K/k)$，从而得到类域论主

定理. 由($A3$)显然有$\mathscr{N}(\mathfrak{M})\subset \mathrm{Ker}\mathscr{A}$,因为$(N\mathfrak{P},K/k)=(\wp,K/k)^{f(\mathfrak{P}|\wp)}=1$. 我们要证明,存在着某些可许模(实际上任意可许模均可),称为 Artin- **导子**,使有

$$P_{\mathfrak{M}}\subset \mathrm{Ker}\mathscr{A},$$

从而

$$P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})\subset \mathrm{Ker}\mathscr{A}$$

即知

$$h=(I(\mathfrak{M}):P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M}))\geqslant \# G=n\ (\text{第一不等式}).$$

但我们已有第二不等式$h\leqslant n$. 这就得到

$$P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})=\mathrm{Ker}\mathscr{A},$$

$$I(\mathfrak{M})/P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})\cong G.$$

先看分圆域情形. 设$K=Q(\zeta_m)$, $k=Q$, $p\nmid m$. $\sigma_p=((p),K/Q)$由其在$\zeta=\zeta_m$上作用决定,而$\sigma_p\zeta\equiv\zeta^p(\mathrm{mod}\mathfrak{P})$等价于

$$\sigma_p\zeta=\zeta^p$$

(§7.4 引理 2). 故对任意$a\in Q$(与m互素正数),则

$$((a),K/Q)\zeta=\zeta^a.$$

故$((a),K/Q)=1\Leftrightarrow a\equiv 1(\mathrm{mod}m)\Leftrightarrow a\equiv 1(\mathrm{mod}^* m\infty)\Leftrightarrow (a)\in P_{m\infty}$,即$P_{m\infty}\subset \mathrm{Ker}\mathscr{A}$. 故$m\infty$即为$Q(\zeta_m)/Q$的 Artin- 导子.

引理 1 设$K\subset k(\zeta_m)$,则K/k的 Artin- 导子存在且仅含m的因子和无限素除子.

证明 $G(k(\zeta)/k)$中元素由其在ζ上作用决定,故问题可化归$Q(\zeta)/Q$. 设$a\in k$与m互素,则$((a),k(\zeta)/k)_{Q(\zeta)}=(N_{k/Q}(a),Q(\zeta)/Q):\zeta\longmapsto\zeta^{|N_{k/Q}(a)|}$, 故$(a)\in \mathrm{Ker}(-,k(\zeta)/k)\Leftrightarrow|N_{k/Q}(a)|\equiv 1(\mathrm{mod}m)$, 只需$N_{k/Q}(a)\equiv 1(\mathrm{mod}^* m\infty)$. 因局部范映射是连续

的，故对每个 $p^e|m$，及 $v=v_p$ 在 k 的延拓 $w=v_{\mathfrak{P}}$，存在 $t(w)$ 使当 $\alpha\in 1+\mathfrak{P}^{t(w)}\subset k_w$ 时，$N_w(\alpha)\in 1+(p)^e$，即 $N_w(\alpha)\equiv 1(\mathrm{mod}\,p^e)$. 取 $\mathfrak{M}=\prod\limits_{v|m}\prod\limits_{w|v}w^{t(w)}\infty$（其中 ∞ 是 k 的所有实无限素除子之积），则知当 $\alpha\equiv 1(\mathrm{mod}^*\mathfrak{M})$ 时 $N_k/_Q(\alpha)\equiv 1(\mathrm{mod}^* m\infty)$，即 $P_{\mathfrak{M}}\in \mathrm{Ker}(-,k(\zeta)/k)\subset \ker(-,K/k)$. □

定理 2 设 K/k 为数域的 n 次 Abel 扩张，则 K/k 的可许模即为其 Artin 导子. 也就是说，若 $\boldsymbol{f}$ 是 K/k 的导子（即最小可许模），模 $\mathfrak{M}$ 是 $\boldsymbol{f}$ 的倍，则 $P_{\mathfrak{M}}\subset\mathrm{Ker}(-,K/k)$，从而 $P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})=\mathrm{Ker}(-,K/k)$，$I(\mathfrak{M})/P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})\cong G(K/k)$.

引理 2 设 K/k 是循环扩张，则 Artin- 导子 $\mathfrak{M}$ 存在且仅含分歧的素除子（最小可许模即导子 $\boldsymbol{f}$ 就可作 Artin- 导子）.

定理 2 的证明 先设 $\mathfrak{M}$ 与 $\boldsymbol{f}$ 有相同的素因子，则 $P_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})=P_f\mathscr{N}(f)$（§9.3）. 设 $K=K_1\cdots K_r$，K_i/k 循环. 由引理 2 知有模 $\mathfrak{M}_i$ 使 $(P_{m_i},K_i/k)=1$ 且 $\mathfrak{M}_i$ 仅含在 K_i 分歧的 v，于是 v 在 K 分歧，故 $v|\boldsymbol{f}$. 故有 t 使 $\mathfrak{M}_i|\boldsymbol{f}^t$. 故 $(\boldsymbol{P}_{f^t},K/k)_{K_i}=(\boldsymbol{P}_{f^t},K_i/k)\subset(\boldsymbol{P}_{\mathfrak{M}_i},K_i/k)=\{1\}$. 故 $\mathrm{Ker}\mathscr{A}_{\mathfrak{M}}\supset \boldsymbol{P}_{f^t}\mathscr{N}(\boldsymbol{f}^t)=\boldsymbol{P}_f\mathscr{N}(\boldsymbol{f})=\boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$. 而对一般的 $\mathfrak{M}$，$\mathrm{Ker}\mathscr{A}_{\mathfrak{M}}=\boldsymbol{I}(\mathfrak{M})\cap\mathrm{Ker}\mathscr{A}_f=\boldsymbol{P}_f\mathscr{N}(\boldsymbol{f})\cap\boldsymbol{I}(\mathfrak{M})=\boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$. 证毕. □

最后只需证明引理 2. 由上节定理 4，只需再证 $\mathrm{Ker}\mathscr{A}\subset\boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$. 这可由已知的分圆扩张结果证出. 以 $\rho_{\mathfrak{M}}(a)$ 记最小正整数 ρ 使 $a^\rho\equiv 1(\mathrm{mod}\mathfrak{M})$. 下面是范·德·瓦尔登的两个初等引理.

引理 3 对任意正整数 $a>1$ 和素数幂 q^r，存在素数 p 使 $\rho_p(a)=q^r$.

证明 $T=(a^{q^r}-1)/(a^{q^{r-1}}-1)=X^{q-1}+qX^{q-2}+\cdots+q$，$X=a^{q^{r-1}}-1$. 取 $p\mid T$，若 $p\nmid X$ 则证毕. 若 $p\mid X$，则 $p\mid q$，$p=q$. 若 $q\neq 2$，则 $q^2\mid X^{q-1}$，$T\equiv q(\bmod q^2)$，$q^2\nmid T^2$. 因 $T>q$，故存在 $p_1\mid \frac{T}{q}$，使 $p_1\nmid X$（否则 $p_1=q$，$q^2\mid T$），此 p_1 即所欲求. 若 $q=2$，则 $T=X+2$，X 偶，a 奇，$X\equiv 0(\bmod 4)$，$2^2\nmid T$. 如上知存在 $p_1\mid T/2$，$p_1\nmid X$，p_1 即合乎要求. □

引理 4 对任意正整数 $a>1$，$n=q_1^{r_1}\cdots q_s^{r_s}$（素分解），存在正整数 $m=p_1\cdots p_s p_1'\cdots p_s'$ 及 b 使 $n\mid\rho_m(a)$，$n\mid\rho_m(b)$，且 p_i 和 p_i' 可为任意大互异素数（$i=1,\cdots,s$），a 与 b 模 m 独立（即在 $(\mathbf{Z}/m\mathbf{Z})^*$ 中生成的子群的交平凡）.

证明 在引理 3 中令 $r\to\infty$，可得任意大 p 使 $q^{r_0}\mid\rho_p(a)$. 故先求大的 $p_1,\cdots,p_S$ 使 $\rho_{p_i}(a)=q_i^{r_i^*}$，$r_i^*>r_i$. 再求大 $p_1',\cdots,p_S'$ 使 $\rho_{p_i'}(a)=q_i^{r_i'}$，$r_i'>r_i^*$. 令 $m=p_1\cdots p_S p_1'\cdots p_S'$. 则 $\rho_m(a)$ 可被 n 整除. 取正整数 b 使 $b\equiv a(\bmod p_1\cdots p_S)$，$b\equiv 1(\bmod p_1'\cdots p_S')$. 则 $n\mid\rho_m(b)$. 再设 $a^\nu b^\mu\equiv 1(\bmod m)$，$\nu,\mu$ 为正整数，则 $a^\nu\equiv 1(\bmod p_1'\cdots p_S')$，故 $(q_1^{r_1'}\cdots q_S^{r_S'})\mid\nu$，从而 $a^\nu\equiv 1(\bmod p_1\cdots p_S)$，$a^\nu\equiv 1(\bmod m)$. 故 $b^\mu\equiv 1(\bmod m)$. □

引理 5 设 K/k 为数域 Abel n 次扩张，S 为有限素数集，$\wp$ 为 k 的素理想且在 K 不分歧，则存在整数 m，与 S 中数及 $\wp$ 互

素，使

(i) $n \mid (\wp, k(\zeta_m)/k)$ 的阶.

(ii) $K \cap k(\zeta_m) = k$.

(iii) 存在 $\tau \in G(k(\zeta_m)/k)$ 与 $(\wp, k(\zeta_m)/k)$ 互相独立，且 n 整除 τ 的阶.（σ 与 τ 独立是指它们生成的子群的交平凡）.

证明 令 $a = N\wp$ 用引理 4，可取 m 只被很大素数整除，从而 $K \cap Q(\zeta_m) = Q$ 而得(ii). 记 $\sigma = (\wp, k(\zeta_m)/k)$，则 $\sigma\zeta = \zeta^a$，得(i). 如在引理 4 中取 b 令 τ 为 $\tau\zeta = \zeta^b$，则得(iii).（$\zeta = \zeta_m$）. □

引理 6(Artin) 设 K/k 为数域 n 次循环扩张，S，$\wp$ 如引理 5，则存在整数 m 与 S 中数互素，存在有限扩张 E/k，使(1) $K \cap E = k$；(2) $K(\zeta_m) = E(\zeta_m)$，$K \cap k(\zeta_m) = k$；(3) $\wp$ 在 E 完全分裂.

证明 取 m 如引理 5，记 $\zeta = \zeta_m$. 则 $G' = G(K(\zeta)/k) = G(K/k) \times G(k(\zeta)/k)$. 设 $G = G(K/k) = \langle\sigma\rangle$，$\tau$ 如引理 5，H 是 G' 中 $\sigma \times \tau$ 和 $(\wp, K/k) \times (\wp, k(\zeta)/k)$ 生成的子群. 故 $H \supset (\wp, K(\zeta)/k)$，从而 H 含 $\wp$ 在 $K(\zeta)$ 的分解群. 记 E 为 H 的固定子域，则 $\wp$ 在 E 完全分裂. 另一方面，显然 $H \cap G \times 1 = \{1\}$. $G \times 1 \subset G'$ 固定 $k(\zeta)$，故 $k(\zeta)E = E(\zeta) = K(\zeta)$. □

引理 2 的证明 设 f 是 K/k 的导子（最小可许模），$I \in \boldsymbol{I}(f)$ 且 $(I, K/k) = 1$. 已知 f 只含分歧素除子，故只需证 $I \in \boldsymbol{P}_f\mathcal{N}(f) = H$，从而 $\mathrm{Ker}\mathscr{A} \subset H$，再由上节定理 4 即得引理. 分解 $I = \wp_1^{c_1} \cdots \wp_r^{c_r}$. 对每个 $\wp_i$，作域 E_i 如引理 6（$\zeta = \zeta_i = \zeta_{m_i}$），取互素的 $m_1, \cdots, m_r$ 含大素因子，则 $K(\zeta_1, \cdots, \zeta_r)/k$ 的 Galois 群为 $G \times G_1 \times \cdots \times G_r$，$G_i = G(Q(\zeta_i)/Q)$. E_i 是 $H_i \times G_1 \times \cdots \times \hat{G}_i$

$\times \cdots \times G_r$ 固定域($\hat{G}_i$ 表示去掉 G_i),$H_i \subset G \times G_i$ 由 $\sigma \times \tau_i$ 和 $(\wp_i, K/k) \times (\wp_i, k(\zeta_i)/k)$ 生成,$G = \langle\sigma\rangle$.

断言:$E = E_1 \cdots E_r$ 使 $K \cap E = k$, 从而 $G(K/k) \cong G(KE/E)$.事实上,E 是诸 $G(KE/E_i)$ 交群的固定域,此交群含 $\sigma \times \tau_1 \times \cdots \times \tau_r$.而 K 被 $1 \times \tau_1 \times \cdots \times \tau_r$ 固定,故 $K \cap E$ 被 $\sigma \times 1 \times \cdots \times 1$ 固定,故必为 k.断言得证.令$(\wp_i^{c_i}, K/k) = \sigma^{d_i}$,某 $d_i \geqslant 0$,则$(I, K/k) = \prod_i \sigma^{d_i} = \sigma^{d_1+\cdots+d_r} = 1$,故$\sum d_i = dn$,$n = [K:k]$.取 E 的分式理想 b_E,与 $\boldsymbol{f}$ 和诸 m_i 互素,使$(b_E, KE/E) = \sigma$(由定理 1).视 $G(K/k) = G = G(KE/E)$.令 $b = N_{E/k}b_E$,则$(b, K/k) = \sigma$.注意 $\wp_i^{c_i}b^{-d_i}$ 是 E_i 到 k 的范,这是由于 $\wp_i$ 在 E_i 完全分裂。设 $\wp_i^{c_i}b^{-d_i} = N_{E_i/k}I_i$,$I_i$ 与 $\boldsymbol{f}$ 和诸 m_i 互素.因$(\wp_i^{c_i}b^{-d_i}, K/k) = 1$,故$(I_i, KE_i/E_i) = 1$.因 KE_i/E_i 是分圆扩张,适用引理 1.记 $I_i = (\beta_i)N_{KE_i/E_i}(B_i)$,理想 B_i 与 $\boldsymbol{f}$ 和 m_i 互素,$\beta_i \equiv 1(\operatorname{mod}^* m\mathfrak{M}_i')$,$\mathfrak{M}_i'$ 是 E_i 的模且含 $\boldsymbol{f}$ 中因子的高次幂和无限素除子.取 E_i 到 k 的范则 $\wp_i^{c_i}b^{-d_i} = (N_{E_i/k}\beta_i)N_{K/k}(N_{KE_i/K}B_i)$,$N_{E_i/k}(\beta_i) \equiv 1(\operatorname{mod}^* \boldsymbol{f})$.对 $i = 1, \cdots, r$ 取积则得 $Ib^{-dn} \in \boldsymbol{P}_{\boldsymbol{f}}\mathcal{N}(\boldsymbol{f})$.$b^{-dn}$ 也是一范,故 $I \in \boldsymbol{P}_{\boldsymbol{f}}\mathcal{N}(\boldsymbol{f})$. □

§9.8 类域论基本定理

9.8.1 类域论基本定理(理想语言)

定理 1(类域论基本定理) 设 K/k 为数域的 n 次 Abel 扩张,$G = G(K/k)$.则存在 k 的模 $\boldsymbol{f}$(称为 K/k 的导子),使得如下成立:

1.对 k 的任意模 $\mathfrak{M}$,若 $\boldsymbol{f} | \mathfrak{M}$,则 Artin 映射

$$\mathscr{A}: \boldsymbol{I}(\mathfrak{M}) \longrightarrow G(K/k), \quad I \longmapsto (I, K/k)$$

的核为 $H = \boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$，从而有群同构（同构定理）：

$$\boldsymbol{I}(\mathfrak{M})/\boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M}) \cong G(K/k),$$

其中 $\boldsymbol{I}(\mathfrak{M}) = \boldsymbol{I}_k(\mathfrak{M})$ 为与 $\mathfrak{M}$ 互素的 k 的（分式）理想构成的群，$\mathscr{N}(\mathfrak{M})$ 为 $\boldsymbol{I}_K(\mathfrak{M})$ 到 k 的范，$\boldsymbol{P}_{\mathfrak{M}}$ 为满足 $\alpha \equiv 1(\mathrm{mod}^{\cdot}\mathfrak{M})$ 的 $\alpha \in k$ 生成的主理想群.

Ⅱ（分歧定理） k 的素除子 v（有限或无限）在 K 分歧当且仅当 $v|f$.

Ⅲ（分裂定理） k 的与 $\mathfrak{M}$ 互素的素理想 $\wp$ 在 K 完全分裂当且仅当 $\wp \in H = \boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M}) = \mathrm{Ker}\mathscr{A}$.

Ⅳ（分解定理） k 的与 $\mathfrak{M}$ 互素的素理想 $\wp$ 在 K 中素分解为 $\wp O_K = \mathfrak{B}_1 \cdots \mathfrak{B}_g$，其中剩余类次数 $f = f(\mathfrak{B}_i | \wp)$ 是使 $\wp^f \in H$ 的最小正整数 $f(i = 1, \cdots, g)$，于是 $fg = n = [K : k]$.

定理 2（存在定理） 设 $\mathfrak{M}$ 为数域 k 的任一模. 对任意满足 $\boldsymbol{I}(\mathfrak{M}) \supset H \supset \boldsymbol{P}_{\mathfrak{M}}$ 的中间群 H，存在唯一的 Abel 扩张 K/k 使得 $H = \boldsymbol{P}_{\mathfrak{M}}\mathscr{N}(\mathfrak{M})$，从而如定理 1 有 Artin 同构 $\boldsymbol{I}(\mathfrak{M})/H \cong G(K/k)$.

定理 2 中的域 K 称为群 H 的（模 $\mathfrak{M}$）**类域**（classfield）. 特别 $\boldsymbol{P}_{\mathfrak{M}}$ 的类域称为**射线类域**（ray class field）. 注意类域为射线类域的子域. 于是由定理 1－2 知，模 $\mathfrak{M}$ 的诸类域（即射线类域的诸子域）K 与 $\boldsymbol{I}(\mathfrak{M}) \supset \boldsymbol{P}_{\mathfrak{M}}$ 的诸中间子群 H 间 1∶1 对应. 若 K_i 与 H_i 对应，则 $K_1 \supset K_2 \Leftrightarrow H_1 \subset H_2$，$K_1K_2$ 与 $H_1 \cap H_2$ 对应（Galois 理论）. 定理 2 证明留下节.

定理 1 的证明 Ⅰ. 上节已证. Ⅱ. 见 §9.3 定义 1 下说明及

§9.6定理2.Ⅲ是Ⅳ推论.Ⅳ.因$(\wp,K/k)$的阶为f,即使$1=(\wp,K/k)^f=(\wp^f,K/k)\Leftrightarrow \wp^f\in H$成立的最小正整数$f$. □

注记 分解定理可推广到在K分歧的k的素理想$\wp$.这时,$\wp$(在K的任一素因子$\mathfrak{B}$)的分解域K^d是$\wp$的最大非分歧子扩张.记K^d/k对应的理想子群为H^d(H^d可刻画为含H的且其类域在$\wp$不分歧的最小理想群),则$\wp$在K分解为

$$\wp O_K=(\mathfrak{B}_1\cdots\mathfrak{B}_g)^e$$

其中$e=(H^d:H)$,$f=f(\mathfrak{B}_i|\wp)$是使$\wp^f\in H^d$的最小正整数,$efg=[K:k]$.(上述H是Abel扩张K/k对应的理想群).

9.8.2 类域论基本定理(idele语言)

设K/k为n次Abel扩张,$G=G(K/k)$,$\mathfrak{f}$为其导子(即最小可许模),$\mathfrak{M}$为其可许模(即$\mathfrak{f}|\mathfrak{M}$).由§9.3有群同构

$$C_k/NC_K\overset{\alpha}{\cong}\boldsymbol{J}_k/k^*N\boldsymbol{J}_K\xrightarrow{\varphi}\boldsymbol{J}_{\mathfrak{M}}/k_{\mathfrak{M}}W_{\mathfrak{M}}N\boldsymbol{J}_K(1,\mathfrak{M})$$
$$\xrightarrow{\psi}\boldsymbol{I}(\mathfrak{M})/P\mathscr{N}(\mathfrak{M})\xrightarrow{\mathscr{A}}G.$$

映射可刻画为:$\forall a\in\boldsymbol{J}_k$,取$\alpha\in k^*$使$\alpha a\equiv1(\mathrm{mod}^*\mathfrak{M})$,则$\varphi(a)=\alpha a$(所在类).$\psi(\alpha a)=(\alpha a)$为$\alpha a$决定的理想(所在类).而$\mathscr{A}(\alpha a)=((\alpha a),K/k)$.因此定义作用于idele的Artin符号为

$$(a,K/k)==((\alpha a),K/k).$$

于是有群同构(**Artin互反律**):

$$\mathscr{A}:\boldsymbol{J}_k/k^*N_{K/k}\boldsymbol{J}_K\xrightarrow{\simeq}G(K/k)$$
$$a\longmapsto(a,K/k).$$

当$\alpha\in k^*\subset\boldsymbol{J}_k$时,显然$(\alpha,K/k)=1$.故$\mathscr{A}$也引起idele类群的商群$C_k/N_{K/k}C_K$与$G(K/k)$的同构.

设$a=(a_v)\in\boldsymbol{J}_k$,每个分量等同于一个idele:

$$a_v = (\cdots, 1, a_v, 1, \cdots) \ (a_v \text{ 为 } v\text{- 分量}).$$

于是 $a = (a_v) = \prod_{v \in M_k} a_v$，故 Artin 符号可分解为：

$$(a,\ K/k) = \prod_{v \in M_k} (a_v,\ K/k).$$

注意乘积中只有限多因子非 1，因为当 a_v 是 k_v 的单位且 v 在 K 非分歧时，a_v 是局部范(§9.6)，从而 $(a_v, K/k) = 1$.

定义于 J_k 上的 Artin 符号与定义于理想上的 Artin 符号自然有类似性质(见 §9.7)：

$(A1')$. 设 $\tau: K \longrightarrow \tau K$ 为域同构(不一定固定 k)，则

$$(\tau a, \tau K/\tau k) = \tau(a, K/k)\tau^{-1}.$$

$(A2')$. 设 $L \supset K \supset k$ 为 Abel 扩张，则在 K 的限制

$$(a, L/k)_K = (a, K/k).$$

$(A3')$. 设 k'/k 为有限扩张，$\boldsymbol{A}$ 为 k 的最大 Abel 扩张，则

$$(a, \boldsymbol{A}/k') = (N_{k'/k} a, \boldsymbol{A}/k)$$

$$(a, Kk'/k')_K = (N_{k'/k} a, K/k).$$

定理 3(类域论基本定理)　设 K/k 为数域的 n 次 Abel 扩张. 则由 Artin 映射引起群的同构映射：

$$C_k/NC_K = \boldsymbol{J}_k/k^* N\boldsymbol{J}_K \xrightarrow{\mathscr{A}} G(K/k),$$

其中 $\mathscr{A}(a) = (a, K/k) = \prod_{v \in M_k} (a_v, K/k)$，　$N = N_{K/k}$，　$\boldsymbol{J}_k$ 为 k 的 idele 群，$C_k = \boldsymbol{J}_k/k^*$ 为 idele 类群.

$N\boldsymbol{J}_K$ 显然是 $\boldsymbol{J}_k$ 的开子群(因 $N_w U_w$ 在 U_v 中指数为 e，故是 U_v 的开子群). 故定理 3 是说，任一 Abel 扩张 K/k 对应 C_k 的一个开子群 $H = NC_K$(或 $\boldsymbol{J}_k \supset k^*$ 的中间开子群 $H = k^* N\boldsymbol{J}_K$). 反之，

我们将证明(存在性定理):对任一开子群 H,总有 Abel 扩域 K/k 使 $H = NC_K$(或 $H = k^* NJ_K$). 这时,对应的 K 和 H 记为 $K(H)$ 和 $H(K)$,分别称为(属于)H 的**类域**和(属于)K 的**类群**.

定理 4 数域 k 的诸有限 Abel 扩张 K/k 与 C_k 的诸开子群 H(或 $J_k \supset k^*$ 的诸中间开子群 H)之间 1:1 对应,其中 K 对应于 $H = N_{K/k}C_K = \mathrm{Ker}\mathscr{A}$(或 $H = k^* N_{K/k}J_K$),$G(K/k) \cong C_K/H$(或 J_k/H),且

(i) $K \subset K' \Leftrightarrow H(K) \supset H(K')$,

(ii) $H(KK') = H(K) \cap H(K')$,

(iii) $K(HH') = K(H) \cap K(H')$.

亦即 k 的有限 Abel 扩张格$\{K\}$ 与 C_k 的开子群格$\{H\}$ 之间反向格同构.

性质(i) ~ (iii) 可由 Galois 理论看出. 若 $\mathfrak{M}$ 是 K/k 的可许模(即 $W_{\mathfrak{M}} \subset NJ_K$),则 $H = k^* NJ_K \subset k^* W_{\mathfrak{M}}$,故有

系 1 设 K/k 为数域的 n 次 Abel 扩张,$\mathfrak{M}$ 为其可许模(即 K/k 的导子 $f|\mathfrak{M}$). 记 $K^{\mathfrak{M}}$ 为 $k^* W_{\mathfrak{M}}$ 所属的类域(称为模 $\mathfrak{M}$ 的**射线类域**). 则 $K \subset K^{\mathfrak{M}}$,特别 $K \subset K^f$(即每个 Abel 扩域 K 均是某射线类域 $K^{\mathfrak{M}}$ 的子域).

系 2(Kronecker-Weber) 每个 Abel 数域 K/Q 均是某分圆域 $Q(\zeta_m)$ 的子域. 事实上,$Q(\zeta_m)$ 是模 $\mathfrak{M} = m\infty$ 的射线类域,亦即是 $Q^* W_{m\infty}$ 的类域. (m 为正整数).

证明 只要证明后一事实, 即 $Q^* W_{m\infty} = \mathrm{Ker}(-,$

$\boldsymbol{Q}(\zeta)/\boldsymbol{Q}$)(在 $\boldsymbol{J}_{\boldsymbol{Q}}$ 中 $\zeta=\zeta_m$),由 §9.3 这相当于 $\boldsymbol{P}_{m\infty}=\mathrm{Ker}(-,\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$(在 $I(m\infty)$ 中),这在上节引理1前或 §9.3末已证. 以下给出新证明,使 Artin 映射更清楚.

先设 $m=p^s$ 为素数 p 的幂,只有 p 和 ∞ 在 $L_m=\boldsymbol{Q}(\zeta_m)$ 分歧,故 $\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$ 可许的模只能形如

$$\mathfrak{M}=p^t\infty \qquad (\text{取 } t\geqslant s).$$

故

$$W_{\mathfrak{M}}(v)=\begin{cases}1+(p)^t, & \text{当 } v=p\\ \boldsymbol{R}^+, & \text{当 } v=\infty\\ U_v, & \text{当 } v\nmid\mathfrak{M}.\end{cases}$$

若 $a=(a_v)\in W_{\mathfrak{M}}$ 则 $(a,\mathrm{L_m}/\boldsymbol{Q})=\prod\limits_v(a_v,L_m/\boldsymbol{Q})=(a_p,L_m/\boldsymbol{Q})(a_\infty,L_m/\boldsymbol{Q})=(a_p,L_m/\boldsymbol{Q})$,这是因为当 $v\neq p,\infty$ 时,v 在 L_m 非分歧,故 $a_v(\in U_v)$ 是局部范,$(a_v,L_m/\boldsymbol{Q})=1$;而 $a_\infty\in\boldsymbol{R}^+$ 是正实数,是任意次幂,$(a_\infty,L_m/\boldsymbol{Q})\in G(L_m/\boldsymbol{Q})$ 是有限阶,故为1. 而对于 U_p 的任一单位 u,视为 $u=(\cdots,1,u,1,\cdots)\in\boldsymbol{J}_{\boldsymbol{Q}}$,取自然数 α 使 $\alpha u\equiv1(\mathrm{mod}\,p^t)$,则 $\alpha u=(\cdots,\alpha,\alpha u,\alpha,\cdots)\in\boldsymbol{J}_{\mathfrak{M}}$. 注意理想 $(\alpha)=(\alpha u)$ 的范数为 α(事实上 $N(\alpha u)=N(\alpha)N(a)=\alpha$ 因 α 是主理想,$(u)=(1)$),故 $\sigma_u=(u,\mathrm{L_m}/\boldsymbol{Q})=((\alpha),\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$ 作用为

$$\sigma_u(\zeta_m)=\zeta_m{}^{\alpha}=\zeta^{u^{-1}}.$$

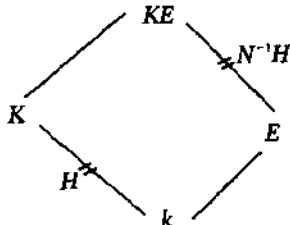
特别当 $u=a_p$ 时,因 $a_p\in W_{\mathfrak{M}}(p)=1+(p)^t\equiv1(\mathrm{mod}\,p^S)$ 知 $\alpha\equiv1(\mathrm{mod}\,p^S)$. 故若 $a\in W_{\mathfrak{M}}$ 则

$$(a,\mathrm{L_m}/\boldsymbol{Q})=(a_p,\mathrm{L_m}/\boldsymbol{Q})=1,$$

即知 $W_{\mathfrak{M}}\subset\mathrm{Ker}(-,\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$.

对一般的 m,由 Artin 符号的积性立得 $W_{m\infty}\subset\mathrm{Ker}(-,\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$. 因我们已知 $\boldsymbol{J}_{\boldsymbol{Q}}/\mathrm{Ker}(-,\boldsymbol{Q}(\zeta)/\boldsymbol{Q})\cong G(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})\cong$

$(\mathbf{Z}/m\mathbf{Z})^* \cong \boldsymbol{I}(m)/\boldsymbol{P}_{m\infty} \cong \boldsymbol{J}_Q/\boldsymbol{Q}^*W_{m\infty}$，故知 $\boldsymbol{Q}^*W_{m\infty} = \mathrm{Ker}(-, \boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$，即 $\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$ 是模为 $m\infty$ 的射线类域. □

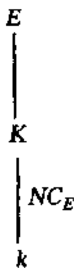


定理 5（平移定理） 设 K/k 是 H 的类域，则 KE/E 是 $N_{E/k}^{-1}(H)$ 的类域，这里 E/k 是任意有限扩域.

证明 $(a, KE/E) = 1$
$\Leftrightarrow (a, KE/E)_K = 1$
$\Leftrightarrow (N_{E/k}a, K/k) = 1 \Leftrightarrow N_{E/k}a \in H$.

定理 6（通用范定理） 设 E/k 是任意有限扩域（不必是 Abel 扩域），则 $N_{E/k}C_E$ 的类域是 E/k 的最大 Abel 子扩域.

证明 设 NC_E 的类域为 K. 由平移定理知 $N^{-1}(NC_E) = C_E$ 的类域为 KE/E，但 C_E 的类域应为 E，故 $K \subset E$. 反之，设 K' 是 E 的 Abel 子扩域，则 $N_{K'/k}C_{K'} \supset N_{E/k}C_E$，故 $K' \subset K$. □



系 3 设 K/k 是有限扩域 E/k 的最大 Abel 子扩域，则(i) $N_{E/k}C_E = N_{K/k}C_K$；(ii) $(C_k : N_{E/k}C_E) = [K : k]$；(iii) $(C_k : N_{E/k}C_E) = [E : k]$ 当且仅当 E/k 是 Abel 扩张.

证明 (i) 二者有相同的类域 K. 其余由此得. □

9.8.3 无限扩张形式的类域论

由于 Artin 符号对扩域的稳定性(A2)，故可对 k 的最大 Abel 扩域 $\boldsymbol{A}$ 定义 Artin 符号(§9.1). 对 idele 上的 Artin 符号也可同样定义：$(-,\boldsymbol{A}/k)$ 在有限 Abel 扩域 K/k 上的限制 $(-,\boldsymbol{A}/k)_K=(-,K/k)$. 于是 $(-,\boldsymbol{A}/k)=\mathscr{A}$ 引起 Artin 映射

$$\mathscr{A}:\quad C_k\longrightarrow G(\boldsymbol{A}/k)=G.$$

把 $G(\boldsymbol{A}/k)$ 的指数有限的子群 H 全体定义为 1 的基本邻域系，从而在 $G(\boldsymbol{A}/k)$ 中引入拓扑(Krull **拓扑**)，$G(\boldsymbol{A}/k)$ 成为拓扑群(对群运算连续). 于是

$$G=G(\boldsymbol{A}/k)=\varprojlim_{G/H\text{有限}}G(\boldsymbol{A}/k)/H=\varprojlim_{K/k\text{有限Abel}}G(K/k).$$

一个拓扑群 G 的闭子群称为其(拓扑)子群(其陪集之积仍为陪集)，G 的开子群也是闭子群(等于其陪集之并的余集). 按 Galois 理论的基本定理有：

Galois 基本定理 $\boldsymbol{A}/k$ 的诸子扩域 K/k 与 G 的诸闭子群 H 间 1∶1 对应，即 $H=G(\boldsymbol{A}/K)$，$G(K/k)=G/H$，K 为 H 的固定子域. 在此对应下，G 的诸开子群 H 与诸有限子扩域 K/k 间 1∶1 对应.

易证 $\mathscr{A}:C_k\longrightarrow G$ 是满射. 首先 $\mathscr{A}C_k$ 在 G 处处稠密：对 G 中 1 的任一开邻域 H(即指数有限子群)，设其固定子域为(有限)扩域 K/k，则 $\mathscr{A}$ 的象在 $G(K/k)=G/H$ 中是满的，故 $1\cdot H\in G/H$ 含 $\mathscr{A}$ 的象. 其次，$\mathscr{A}C_k$ 是紧的：体积为 1 的 idele 集 $\boldsymbol{J}_k^0\supset k^*$(§9.1)，故每个 idele 类中的 idele 有相同体积. 对正实数 $\rho\in\boldsymbol{R}^+$ 令 $a_\rho=(\rho^{\frac{1}{n}},\cdots,\rho^{\frac{1}{n}},1,1,\cdots)$(仅在无限素除子分量非 1)，则任一 idele 可分解为 $a=a_\rho a^0$，$a^0\in\boldsymbol{J}_k^0$. 故 $C_k\cong\boldsymbol{R}^+\times C_k^0$. 因 a_ρ 可任意次开方，故 $\mathscr{A}(\boldsymbol{R}^+)=\{1\}$. 显然 C_k^0 与 $\mathscr{A}C_k^0$ 均紧，故

$\mathscr{A}C_k$ 紧.因此可知上述 Artin 映射 $\mathscr{A}$ 为满射.

注意$(a,\boldsymbol{A}/k)=1\Leftrightarrow(a,K/k)=1$($\forall$ 有限子扩张 K/k)$\Leftrightarrow a\in H_K$(即 K 在 $G(\boldsymbol{A}/k)$ 中固定子群). 故

$$H_A=\mathrm{Ker}(-,\boldsymbol{A}/k)=\bigcap_{K/k\text{有限}}H_K,$$

$$H_K=\mathrm{Ker}(-,K/k)=\bigcap_{\substack{F/k\text{有限}\\K\supset F}}H_F.$$

定理 7(类域论基本定理 —— 无限扩张形式) 数域 k 的诸 Abel 扩张 K/k(有限或无限)与 idele 类群 C_k 的含 H_A 闭子群 H 之间 1∶1 对应,这里 $H=\mathrm{Ker}(-,K/k)=G(\boldsymbol{A}/K)=\bigcap H_F(K\supset F,F/k$ 有限),且若 K_i 与 H_i 对应则 $K_1\subset K_2\Leftrightarrow H_1\supset H_2$, K_1K_2 对应于 $H_1\cap H_2$,$K_1\cap K_2$ 对应于 H_1H_2. 而且在上述对应中,有限 Abel 扩张 K/k 与开子群 H 间 1∶1 对应.

§9.9 存在 — 分裂 — 分歧定理

定理 1(存在定理) 设 $\boldsymbol{J}_k$ 是数域 k 的 idele 群,H 是 $\boldsymbol{J}_k$ 的任一含 k^* 开子群,则存在属于 H 的类域 K(即存在有限 Abel 扩域 K/k 使 $H=k^*N_{K/k}\boldsymbol{J}_K$).

引理 1(递归引理) 设 H 是 J_k 的含 k^* 开子群. 若对某循环扩张 E/k,$N_{E/k}^{-1}(H)$ 有类域 L/E,则 H 有类域 K/k. (此引理可视为平移定理之逆)

证明 先证 L/k 是 Galois 扩张. 设 L'/k 是含 L 的最小 Galois 扩张,$\sigma\in G(L'/k)$. 记 $H_E=N_{E/k}^{-1}(H)$,则 $\sigma H_E=H_E$. 因 σL 是 σH_E 的类域,故 $\sigma L=L$,L/k 为 Galois 扩张,从而 $L'=L$.

设 $\sigma \in G(L/k)$ 在 E 的限制生成 $G(E/k)$，$\tau \in G(L/E)$，$\tau = (b, L/E)(b \in J_E)$. 则 $\sigma\tau\sigma^{-1} = (\sigma b, \sigma L/\sigma E) = (\sigma b, L/E)$. 由 $N_{E/k}(\sigma b/b) = 1$ 知 $\sigma b/b \in H_E$，$(\sigma b, L/E) = (b, L/E)$，$\sigma\tau\sigma^{-1} = \tau$. 故 L/k 为 Abel 扩张. 由 $k^* N_{L/k} J_L \subset H$，设 K 是 $(H, L/k)$ 的固定子域，由 Artin 映射稳定性可知，H 是 $\mathscr{A}: C_k \longrightarrow G(K/k)$ 的核，故 K 是 H 的类域. □

递归引理可将定理 1 化为 k 含 ζ_n 情形，这里记 J_k/H 的指数为 n（即元素的 n 次方均为 1）：令 $E = k(\zeta_n)$，则必有循环扩张塔

$$k \subset E_1 \subset E_2 \subset \cdots \subset E_r = E,$$

E_{i+1}/E_i 均循环. 令 $H_i = N_{E_i/k}^{-1}(H)$，若能证明 $H_r = H_E$ 有类域，则由递归引理可依次下推，知 H 有类域.

引理 2 设 n 次本原单位根 $\zeta_n \in k$，S 是 k 的素除子集，含所有无限素除子及 n 的素因子，且使 $J_k = k^* J_S$. 设 $B = \prod\limits_{v \in S} k_v^{*n} \times \prod\limits_{v \notin S} U_v$，则 $k^* B$ 有类域 $K = k(k_S^{\frac{1}{n}})$，且 $[K : k] = n^{|S|}$，$k^* \cap B = k_S^n$（k_S 为 S- 单位，见 §9.1）.

定理 1 的证明 设 J/H 指数为 n，由递归引理可设 $\zeta_n \in k$. 因 J/H 有限，故 H 的分量除有限处外与 J 相同，从而可取有限的 S 使 $v \notin S$ 时 H 的 v- 分量为 U_v，故引理 2 中 $B \subset H$（$\forall a \in J$，$a^n \equiv 1 (\mathrm{mod} H)$，故 $a^n \in H$）. 于是由 $k^* B$ 有类域 K 知 $k^* H = H$ 也有类域（即为 $(H, K/k)$ 的固定子域）. □

引理 2 的证明 主要用 Kummer 扩张理论，含 ζ_n 的 k 的指数为 n 的 Abel 扩张与 $k^* \supset k^{*n}$ 的中间群对应：(1) 设 $k^* \supset D \supset$

k^{*^n} 且 $(D:k^{*^n})$ 有限. 设 $K_D=k(D^{1/n})$ 由添加 D 中所有元素 n 次根而得. 设 D/k^{*^n} 的代表元为 $\alpha_1,\cdots,\alpha_m$ 则 $K_D=k(\alpha_1^{1/n},\cdots,\alpha_m^{1/n})$, 显然 K_D/k 是 Abel 扩张,(群的) 指数为 n. (2) 反之设 K/k 是指数 n 的 Abel 扩张, 则 K 为循环扩张的复合, 每个循环扩张可写为 $k(\alpha^{1/n})$(Hilbert 定理 90, 见 Lang, Algebra). 故 $\mathrm{K}=\mathrm{K}_\mathrm{D}$(某 D). $\mathrm{G(K/k)}$ 与 $\mathrm{D/k^{*^n}}$ 间有如下对偶: 设 $\mathrm{K}=\mathrm{K}_\mathrm{D}$. 对每一 $\sigma\in\mathrm{G(K/k)}=\mathrm{G}$, $\alpha\in\mathrm{D}$; 取 $\mathrm{A}\in\mathrm{K}$ 使 $\mathrm{A}^n=\alpha$. 则 $\sigma\mathrm{A}/\mathrm{A}=\langle\sigma,\alpha\rangle$ 是 n 次单位根且不依于 A 的选取. 映射 $\mathrm{G}\times\mathrm{D}\longrightarrow\boldsymbol{C}^*$, $(\sigma,\alpha)\longrightarrow\langle\sigma,\alpha\rangle$ 是一配对(双积性), 只依于 $\alpha(\mathrm{mod}\,k^{*^n})$, 故诱导出配对 $g:G\times D/k^{*^n}\longrightarrow\boldsymbol{C}^*$. 它是非退化的: (i) 若 $\alpha\in D$ 使 $\langle G,\alpha\rangle=1$ 则 $\alpha^{1/n}\in k$, $\alpha\in k^{*^n}$; (ii) 若 $\sigma\in G$ 使 $\langle\sigma,D\rangle=1$, 对任意 $\alpha\in D$ 若 $A^n=\alpha$ 则 $\sigma A=A$, 故 σ 保 K_D 生成元系不变, $\sigma=1$. g 的非退化说明 G 与 D/k^{*^n} 同构且其子群间对偶. 特别知 $[K_D:k]=(D:k^{*^n})$.

现证引理 2. 设 $K=k(k_S^{1/n})$. 显然 $k_S\cap k^{*^n}=k_S^n$, $k_Sk^{*^n}/k^{*^n}\cong k_S/(k_S\cap k^{*^n})=k_S/k_S^n$. 故 K 是对应于 $k_Sk^{*^n}$ 的 Kummer 扩域(上述). 不计单位根, k_S 是秩为 $s-1$ 自由群 $(s=|S|)$, 故 $(k_S:k_S^n)=n^S=[K:k]$. K/k 在 S 外不分歧: K 由添加 $f(X)=X^n-\alpha$ 根 A 生成 $(\alpha\in k_S)$, $f'(A)$ 仅含 S 中素因子. 对 $v\in S$, $k_v^{*^n}\subset\boldsymbol{J}_k$ 属 $\mathrm{Ker}(-,K/k)$(因 K/k 指数为 n), 故 $k_v^{*^n}\subset k^*N\boldsymbol{J}_K$. 又因 $\prod_{v\notin S}U_v\subset N\boldsymbol{J}_K$(单位范指数定理), 故 $k^*B\subset k^*N\boldsymbol{J}_K$. 事实上二者相等, 仅需证 $(\boldsymbol{J}_k:k^*B)=n^s$. 记 $k_B=k^*\cap B$, 则 $(\boldsymbol{J}_k:k^*B)=(k^*\boldsymbol{J}_S:k^*B)=(\boldsymbol{J}_S:B)/(\boldsymbol{J}_S\cap k^*:B\cap k^*)=\prod_{v\in S}(k_v^*:k_v^{*^n})/(k_S:K_B)=n^{2S}/(k_S:k_B)$, 其中 $(k_v^*:k_v^{*^n})=n^2$

见下面 Artin 引理. 只需再证 $k_B = k_S^n$. 显然 $k_B \supset k_S^n$. 反之取 $\alpha \in k_B$,则 α 在 $v \in S$ 均为局部 n 次幂,故 v 在 $k(\alpha^{1/n})$ 分裂. 而若 $v \notin S$ 则 v 在 $k(\alpha^{1/n})$ 不分歧. 记 $K' = k(\alpha^{1/n})$,则 $J_S \subset N_{K'/k}J_{K'}$,故 $J_k = k^* J_S \subset k^* N_{K'/k}J_{K'}$,由前述类域论知 $K' = k$, $\alpha \in k_S^n$. □

引理 3(Artin) 设 $v = \wp$是$\wp$ — adic 素除子,U 是 k_v 的单位群,n 为正整数, 则 $(U : U^n) = \omega_n / \| n \|_v$, $(k_v^* : k_v^{*n}) = n\omega_n / \| n \|_v$. 特别若 k_v 含 n 次单位根,则 $(U : U^n) = n / \| n \|_v$, $(k_v^* : k_v^{*n}) = n^2 / \| n \|_v$,其中 ω_n 是 k_v 中 n 次单位根个数.

证明 只需证第一个公式(由 $k_v^* \cong \mathbf{Z} \times U$ 知其余). 取 r 使 $|n\pi^{r+1}| \geqslant |\pi^{2r}|$($\pi$ 为 k_v 素元),考虑 $U_r = 1 + \wp^r$. 因 $(1 + a\pi^r)^n = 1 + na\pi^r (\mathrm{mod}\ n\pi^{r+1})$ 对任意整数 $a \in k_v$ 成立,故 $U_r^n = U_{r+s}$, $s = v(m)$(指数赋值). 取 r 足够大使 U_r 不含 n 次单位根($\neq 1$),用三指数引理(§9.5)于 $f: a \to a^n$ 则 $(U:U_r) = (U^m : U_{r+s})\omega_n = (U:U_{r+s})\omega_n / (U:U^m)$. 故 $(U:U^n) = (U:U_{r+s})\omega_n / (U:U_r) = (U_r : U_{r+s})\omega_n$,由 $(U_r:U_{r+s}) = (N\wp)^s$ 即得引理. □

定理 2 (分裂定理) (1)设 K/k 是 H 的类域($J_k \supset H \supset k^*$),$v$ 是 k的素除子. 则 v 在 K(完全)分裂 $\Leftrightarrow k_v^* \subset H$.

(2) 设 K/k 是 Abel 扩张,v 是 k 素除子. 则

$$(k_v^*, K/k) = G_v.$$

其中 $G_v = G_w$ 是 w 的分解群(w 是 v 到 K 任一延拓).

(3) Artin 映射$(—, K/k) = \mathscr{A}$ 限制到 k_v^* ($\subset J_k$)记为 $\mathscr{A}_v$,则 $\mathrm{Im}\mathscr{A}_v = G_v$, $\mathrm{Ker}\mathscr{A}_v = N_w K_w^*$,故有

$$k_v^* / N_w K_w^* \cong (k_v^*, K/k) = G_v.$$

(N_w 是完备域 K_w 到 k_v 的局部范映射).

证明 (1)若 v 分裂则 $k_v=K_w$,故 k_v^* 中元皆为范,含于 H. 再证其逆,先设 J_k/H 指数为 n, k 含 ζ_n 固定 v_0 使 $k_{v_0}^*\subset H$,设 $S\subset M_k$ 含 v_0,无限 v,n 的因子,分歧的 v 且使 $J=J_k=k^*J_S$. 设 $B_1=k_{v_0}^*\times\prod\limits_{\substack{v\in S\\ v\neq v_0}}k_v^{*n}\times\prod\limits_{v\notin S}V_v$, $B_2=k_{v_0}^{*n}\times\prod\limits_{\substack{v\in S\\ v\neq v_0}}k_v^*\times\prod\limits_{v\notin S}V_v$. 则 $B_1\cap B_2=B$ 如引理 2,$B_1\subset H$. 将构作 k^*B_1 的类域 K_1 且有 v_0 在 K_1 完全分裂,从而由 $K\subset K_1$ 知 v_0 在 K 完全分裂. 设 $D_1=k^*\cap B_1$, $D_2=k^*\cap B_2$. 则 $k_S^n\supset D_1\cap k^{*n}\supset B\cap k^{*n}=k_S^n$(引理 2),故 $D_1\cap k^{*n}=k_S^n$. 同样有 $D_2\cap k^{*n}=k_S^n$. 令 $K_1=k(D_2^{1/n})$,$K_2=k(D_1^{1/n})$,由引理 2 证明(Kummer 理论)知$[K_1:k]=(D_2k^{*n}:k^{*n})=(D_2:D_2\cap k^{*n})=(D_2:k_S^n)$,同样有$[K_2:k]=(D_1:k_S^n)$. 设 K_1,K_2 为 H_1,H_2 的类域,则因 K_1 和 K_2 在 S 外不分歧;$v(\neq v_0)\in S$ 在 K_2 分裂; v_0 在 K_1 分裂,知 $B_1\subset H_1$,$B_2\subset H_2$. 故$[K_1:k]\leqslant(J:k^*B_1)=(k^*J_S:k^*B_1)=(J_S:B_1)/(k_S:k^*\cap B_1)=\prod\limits_{v_0\neq v\in S}(k_v^*:k_v^{*n})(k^*\cap B_1:k_S^n)/(k_S:k_S^n)=\prod\limits_{v_0\neq v\in S}(k_v^*:k_v^{*n})[K_2:k]/n^s$. 同理有$[K_2:k]\leqslant(J:k^*B_2)=(k_{v_0}^*:k_{v_0}^{*n})[K_1:k]/n^s$. 二式相乘得$[K_1:k][K_2:k]\leqslant(J:k^*B_1)(J:k^*B_2)\leqslant[K_1:k][K_2:k]$. 故前述均等号,特别有 $k^*B_1=H_1$. 此情形证毕.

(2) G_v 的固定子域为分解域 K^d,v 在 K^d 分裂,故 $k_v^*\subset N_{K^d/k}J_{K^d}$,即 k_v^* 中元可表为 $a=N_{K^d/k}b$,$b\in K_{w'}^d\subset J_{K^d}(w'|v)$. 故 $(a,K/k)=(b,K/K^d)\in G(K/K^d)=G_v$. 即得$(k_v^*,K/k)\subset G_v$. 欲证二者相等,不妨设 $k=K^d$. 设 E 是 $I=\mathrm{Im}\mathscr{A}_v$ 的固定子域,若 $E\neq k$,则 E 含素数 p 次循环子扩张 F/k,记 $k'=k(\zeta_p)$,$F'=Fk'$

$=F(\zeta_p)$，v'是 v 到 k' 延拓. 则 k_v^{*} 含于 Artin 映射 $k_v^{*}\to G_v(F/k)$ 的核，故 $k'^{*}_{v'}$ 含于 Artin 映射 $k'^{*}_{v'}\to G_{v}'(F'/k')$ 的核. 由(1)已证部分知 v' 在 F' 完全分裂. 而$[k':k]\mid(p-1)$，$p=[F:k]$，二者互素. 因分歧指数和剩余类次数均有积性(对扩张塔)，故 v 在 F 分裂，这与所设 $k=K^d$ 矛盾. 即得(2)，由(2)即得(1).

(3)由于范 $N_wK_w^{*}\subset\mathrm{Ker}\mathscr{A}_v$ 及局部范指数 $k_v^{*}/N_wK_w^{*}=[K_w:k_v]=|G_v|$(§9.6 定理 2)即知 $N_wk_w^{*}=\mathrm{Ker}\mathscr{A}_v$. 其余显然.

□

系 1 $(k_v^{*},K/k)=(K_{w'}^{d*},K/K^d)$，其中 K^d 是 $v\in M_k$ 的分解域，w'是 v 在 K^d 的延拓.

证明($\subset$) 由上述证明知(2)$(a,K/k)=(b,K/K^d)$.

($\supset$)对 $b\in K_{w'}^{d}$，$(b,K/K^d)=(N_{K^d/k}b,K/k)\subset(k_v^{*},K/k)$. □

定理 3(分歧定理) (1)设 K/k 是 H 的类域($J_k\supset H\supset k^{*}$)，$v$ 是 k的素除子. 则 v 在 K 不分歧 $\Leftrightarrow U_v\subset H$(其中 U_v 是 k_v 的单位群).

(2)设 K/k 是 Abel 扩张，v 是 k 的素除子，则

$$(U_v,K/k)=T_v$$

其中 $T_v=T_w$ 是 v 在 K 任一延拓 w 的惯性群.

(3)Artin 映射$(-,K/k)=\mathscr{A}$ 限制于 $U_v(\subset J_k)$记为 $\mathscr{A}_v$，则 $\mathrm{Im}\mathscr{A}_v=T_v$， $\mathrm{Ker}\mathscr{A}_v=N_wU_w$，故

$$U_v/N_wU_w\cong(U_v,K/k)=T_v.$$

证明 先证(3)，由分裂定理知 $N_wK_w^{*}$ 是 $\mathscr{A}$ 在 k_v^{*} 的核. 故若记 H 为 $\mathscr{A}$ 在 J_k 上的核则

$$H \cap k_v^* = N_w K_w^*.$$

于是

$$H \cap U_v = N_w U_w,$$

这是因为 $N_w K_w^* \cap U_v = N_w U_w$，即若 $N_w b$ 为单位则 b 为单位. 故 $\mathscr{A}$ 在 U_v 的核为 $N_w U_w$. 再证其象为 T_v. 由系 1，不妨设 $k = K^d$，即 $G(K/k) = G_v$. 设 K^t 为 T_v 的固定子域，v 到 K^t 延拓为 w'，当 v 有限时有

$$T_v = G(K/K^t) \overset{(1)}{=\!=} (K_{w'}^{t*}, K/K^t) \overset{(2)}{=\!=} (\pi^z \times U_{w'}, K/K^t) \overset{(3)}{=\!=}$$

$$= (U_{w'}, K/K^t) \overset{(4)}{=\!=} (N_w U_w, K/k) \overset{(5)}{=\!=} (U_v, K/k),$$

其中(1)由定理 2，(2)中 π 是 K_w^t 的素元，(3)是因 w 在 K/K^t 完全分歧，故存在 π 为从 K_w 的局部范，(4)因 $N_{K^t/k}(U_{w'}) = N_w U_w$，(5)因 $U_v = N_w U_w$(局部范指数定理). 其余显然. □

§9.10 局部类域论

由上述(整体)类域论可导出局部类域论，即关于局部域扩张的类域论. 局部域是指 $\boldsymbol{Q}_p$ 的(有限)扩张，恰为 $\boldsymbol{Q}$ 的(有限)扩张 K 的局部化 K_w(§5.1 系 2).

设 K/k 是数域的有限扩张，K_w/k_v 是它们的完备化，$w|v$ 分别是 K 和 k(也是 K_w 和 k_v)的素除子. 当 Artin 符号(映射) $\mathscr{A} = (-, K/k)$ 限制到 k_v^* ($\subset \boldsymbol{J}_k$)上时，我们把它记为

$$\mathscr{A}_v = (-, K_w/k_v) = (-, K/k)_{k_v^*},$$

而称为局部 Artin 符号(映射). 由上节定理 2(分裂定理)(3)可知，$\mathscr{A}_v$: $k_v^* \longrightarrow G_v \cong G(K_w/k_v)$ 为满射.

定理 1(局部类域论基本定理) (1)设 K_w/k_v 是局部域的

有限 Abel 扩张，群为 $G(K_w/k_v)=G_v$，分别有素除子 v,w；单位群 U_v,U_w. 则 Artin 映射

$$\begin{aligned}\mathscr{A}_v:\quad k_v^* &\longrightarrow G(K_w/k_v)\\ a &\longmapsto (a,K_w/k_v)\end{aligned}$$

为满射且核 $\mathrm{Ker}\mathscr{A}_v=N_wK_w^*$，从而有群同构

$$k_v^*/N_wK_w^*\cong(k_v^*,K_w/k_v)=\mathrm{Gal}(K_w/k_v),$$

$$U_v/N_wU_w\cong(U_v,K_w/k_v)=T_v$$

其中 T_v 为 K_w/k_v 的分歧群.

(2) k_v 的诸有限 Abel 扩张 K_w/k_v 与 k_v^* 的诸开子群 H 之间 1:1 对应，包含关系相反，其中 K_w 对应于 $H=N_wK_w^*=Ker(-,K_w/k_v)$，$G(K_w/k_v)\cong k_v^*/H$.

(3) K_w/k_v 非分歧$\Leftrightarrow U_v=N_wU_w\Leftrightarrow U_v\subset H\cap N_wK_w^*$.

此时 $G(K_w/k_v)$循环，由 Frobenius 同构 σ 生成，且对 $a\in k_v^*$ 有

$$(a,K_w/k_v)=\sigma^{v(a)}$$

(其中 $v(a)$是标准指数赋值).

证明 (1)与(2)由上节分裂和分歧定理立得. 至于(3)，先回忆 Artin 映射在 J_k 上的作用. 对 $a\in J_k$，取 $\alpha\in k^*$ 使 $\alpha a\equiv 1\ (\mathrm{mod}^*\mathfrak{M})$，再令$(a,K/k)=((\alpha a),K/k)$，其中 $\mathfrak{M}$ 是对 K/k 可许的 k 的任一模. 以下设 $v=v_\wp$，对于 $a=a_v\in k_v^*$，视 $a_v=(\cdots 1,a_v,1,\cdots)\in J_k$ 则$(a_v,K_w/k_v)=(a_v,K/k)$. 设 $a_v=u\pi^r$，$u\in U_v$，$(\pi)=\wp$.

若 K_w/k_v 非分歧(即 v 非分歧)，则 $v\nmid f$(K/k 的导子)，$a_v\in J_f$(即 α 可取为 1，mod^*f 的 v—分量无限制)，于是

$$\begin{aligned}(a_v,K_w/k_v)&=(a_v,K/k)=((a_v),K/k)=(\wp^r,K/k)\\&=(\wp,K/k)^r=\sigma^r.\end{aligned}$$

若 K_w/k_v 分歧(即 v 在 K/k 分歧),则 $v|\boldsymbol{f}$. 取 $\alpha\in k^*$ 使 $\alpha a_v \equiv 1(\bmod^* \boldsymbol{f})$(这相当于 $\alpha a_v\equiv 1(\bmod^* f_v)$),因 $\alpha a_v=(\cdots\alpha,\alpha a_v,\alpha,\cdots)$,理想$(\alpha a_v)\in I(f)$由非 $\boldsymbol{f}$-分量决定,故$(\alpha a)=(\alpha)$,即 $(a_v,K_w/k_v)=((\alpha),K/k)$,故对任意 $x\in K_w$ 有

$$(a_v,K_w/k_v)x\equiv x^{N(\alpha)}(\bmod \mathscr{P}),$$

$\mathscr{P}$ 为 $\wp$ 在 K_w 的素理想因子. □

也可定义无限扩张的 Artin 符号. 设 $\boldsymbol{A}_v$ 是 k_v 的最大 Abel 扩张,$\mathscr{A}_v=(-,\boldsymbol{A}_v/k_v)$如下定义:它在任一有限 Abel 扩张 K_w/k_v 上的限制为$(-,\boldsymbol{A}_v/k_v)_{K_w}=(-,K_w/k_v)$. 于是有 Artin 映射

$$\mathscr{A}_v:\ k_v^* \longrightarrow G=G(\boldsymbol{A}_v/k_v),$$
$$a\longmapsto(a,\boldsymbol{A}_v/k_v).$$

群 k_v^* 与 G 的拓扑都定义为 Krull 拓扑:的开子群为指数有限的子群. 易知 $\mathrm{Ker}\mathscr{A}_v=k_v^*$ 的开子群的交$=1$(因为$\bigcap_r(1+\wp^r)=1$),这点与整体类域论不同,使得局部类域论更简洁. 同样易知 $\mathrm{Im}\mathscr{A}_v$ 在 G 中是处处稠密的,但现 k_v^* 不再是紧的,所以不能得到 $\mathscr{A}_v$ 是满射的结论. 为此把 k_v^* 按 Krull 拓扑完备化. 注意

$$k_v^*=\pi^{\mathbf{Z}}\times U_v=\pi^{\mathbf{Z}}\times W\times U_1$$

其中 π 为 k_v 的素元,W 是单位根群,$U_1=1+\wp$(这是因为 k_v^* 中元为 $\pi^r u$, $u\in U_v$. 而因 $X^{N\wp-1}-1\equiv 0(\bmod\ \wp)$无重根,故由 Hensel 引理知在 k_v 中有 $N\wp-1$ 个互异根,即知 k_v 含 $N\wp-1$ 次单位根群 W. 模 $\wp$引起双射 $W\to\bar{k}_v^*=\boldsymbol{F}_{N\wp}^*$($N\wp$元有限域乘法群,在 U_v 中的核为 $U_1=1-\wp$,故 $U_v=W\times U_1$). 令

$$\hat{k}_v^*=\varprojlim k_v^*/H=\varprojlim(\mathbf{Z}/m\mathbf{Z}\times W'\times U_1/U_1^r)$$
$$=\hat{\mathbf{Z}}\times W\times U_1=\hat{\mathbf{Z}}\times U_v,$$

式中 H 过 k_v^* 开(指数有限)子群,m 过自然数,W'是 W 的商

群，而 $\hat{\mathbf{Z}}=\varprojlim \mathbf{Z}/m\mathbf{Z}$. 显然$\varprojlim U_1/U_1^m=U_1$，故有上式. 由中国剩余(孙子)定理知 $\mathbf{Z}/m\mathbf{Z}=\coprod_p \mathbf{Z}/p^r\mathbf{Z}$，故 $\hat{\mathbf{Z}}=\prod_p \mathbf{Z}_p$. $\mathbf{Z}_p$ 是 p-adic 整数环. 于是 $\mathscr{A}_v:\hat{k}_v^*\longrightarrow G$ 是满射. 故有

定理 2(局部类域论基本定理——无限扩张形式) 设 k_v 是 $\boldsymbol{Q}_p$ 的有限扩张，A_v 是 k_v 的最大 Abel 扩张. 则局部 Artin 映射引起连续同构映射

$$\hat{k}_v^*\cong\hat{\mathbf{Z}}\times U_v\xrightarrow{\mathscr{A}_v}G(A_v/k_v)$$

并建立起诸 Abel 扩张 K/k_v 与 k_v^* 的闭子群 H 间的 1∶1 对应，使

$$\hat{k}_v^*/H\cong G(K/k_v),$$
$$U_v/\bigcap_{F_w}N_wU_w\cong T(K/k_v),$$

式中 F_w 过 K/k_v 的有限子扩张 F_w/k_v，$T(K/k_v)$是惯性群.

例 1 设 $k_v=\boldsymbol{Q}_p$，p 为素数，则 $\pi=p$，$v=p$，$U_p=\boldsymbol{Z}_p^*$，$\boldsymbol{Q}_p^*=p^{\boldsymbol{Z}}\times U_p$. 设 $K=\boldsymbol{Q}_p(\zeta_m)$，$m=np^c$，$c\geqslant 0$，$p\nmid n$. 则 K 为 $K_1=\boldsymbol{Q}_p(\zeta_n)$与 $K_2=\boldsymbol{Q}_p(\zeta_{p^c})$的复合. 对 $\boldsymbol{Q}_p^*$ 中任一元 $a=p^bu$ ($u\in U_p$)，$(a,K/\boldsymbol{Q}_p)$由$(a,K_1/\boldsymbol{Q}_p)$和$(a,K_2/\boldsymbol{Q}_p)$完全决定. 因 p 在 K_1 不分歧，局部单位总是范，故$(u,K_1/\boldsymbol{Q}_p)=1$. 故由定理 1 有

$$(a,K_1/\boldsymbol{Q}_p)=((p^b),K_1/\boldsymbol{Q}_p)=\sigma^b:\qquad \zeta_n\longmapsto\zeta_n^{p^b}.$$

而 K_2 的素元取为 $\pi=1-\zeta_{p^c}$，由 $(X^{p^c}-1)/(X^{p^{c-1}}-1)=(X^{p^{c-1}})^{p-1}+\cdots+1$ 知 $p=\prod_i(1-\zeta_{p^c}^i)=N(\pi)$($i\neq 1$ 与 p 互素)，故$((p),K_2/\boldsymbol{Q}_p)=(N(\pi),K_2/\boldsymbol{Q}_p)=1$，从而由 §9.2 系 2 新证明知

$(a, K_2/Q_p) = ((u), K_2/Q_p)$: $\zeta_{p^c} \longmapsto \zeta_{p^c}^{u^{-1}}$.

故 $U_p \xrightarrow{\mathscr{A}_p} T_p = G(K_2/Q_p)$, $u \longmapsto u^{-1} (\mathrm{mod}\, p^c)$;

而 $W_{p-1} \xrightarrow{\mathscr{A}_p} G(Q_p(\zeta_p)/Q_p)$, $1 + p\mathbf{Z}_p \xrightarrow{\mathscr{A}_p} G(\mathbf{Q}_p(\zeta_{p^c})/Q_p(\zeta_p))$, 均为同构. 取逆向极限知 $Q_p^* = p^{\hat{2}} \times U_p \cong G(Q_p^{ab}/Q_p)$, 且若记 Q_p 的最大 Abel 扩张为 $Q_p^{ab} = Q_p(\zeta_3, \zeta_4, \zeta_5, \cdots) = Q_p(\zeta_{p^\infty}) Q_p(\zeta_{n^\infty})$, $n^\infty = \{0 < n \in \mathbf{Z} \mid (n, p) = 1\}$. 则 $G(Q_p(\zeta_{p^\infty})/Q_p) \cong U_p$, $G(Q_p(\zeta_{n^\infty}/Q_p) \cong p^{\hat{2}}$.

§9.11 Hilbert 类域及例

设 K/k 是 H 的类域($J_k \supset H \supset k^*$), 由分歧定理知 $v \in M_k$ 在 K 非分歧 $\Leftrightarrow U_v \subset H$. 故所有 $v \in M_k$ 在 K 非分歧 $\Leftrightarrow U_v \subset H$ ($\forall\, v \in M_k$) $\Leftrightarrow \prod_{v \in M_k} U_v \subset H$. 注意 $\prod_v U_v = \prod_{v \in S_\infty} k_v^* \times \prod_{v \notin S_\infty} U_v = J_{S_\infty}$, 记为 J_∞.

定义 1 数域 k 的最大非分歧(对所有有限和无限素除子) Abel 扩张 K 称为 k 的 **Hilbert 类域**. (自然 K/k 的导子 $f=1$).

定理 1 对 Abel 扩张 K/k 以下命题等价:

(1) K 是 k 的 Hilbert 类域;

(2) K 是 k 的 idele 子群 $k^* J_\infty$ 的类域;

(3) K 是 k 的主理想子群 $\boldsymbol{P}$ 的类域.

证明 由 K/k 的非分歧性知 K 对应的群 $H \supset k^* J_\infty$, 再由 K/k 的极大性即知 $H = k^* J_\infty$, 得(1)与(2)等价. 而由 $J/k^* J_\infty$

$\cong \boldsymbol{I}/\boldsymbol{P}$ 即得(3)与(2)等价. □

定理 2 设 K 是 k 的 Hilbert 类域,则

(1) $\boldsymbol{J}/k^* \boldsymbol{J}_\infty \cong \boldsymbol{I}/\boldsymbol{P} \cong G(K/k)$.

即 k 的 idele 类群≅理想类群≅Galois 群 $G(K/k)$.

(2) k 的素理想 $\wp$ 在 K 完全分裂⇔$\wp$是主理想. 更一般地, $f(\mathscr{P}|\wp)$是使$\wp^f$ 为主理想的最小正整数 f ($\mathscr{P}$ 为$\wp$在 K 任一素因子).

(3)(主理想定理) k 的任一理想 I 到 K 均为主理想,即 IO_K 为主理想.

证明 (1)和(2)是一般结果的特殊情形.

(3)设 $k \subset K \subset L$, K/k, L/K 均为 Hilbert 类域. 首先, L/k 为 Galois 扩张:若 λ 是 L 到 $\boldsymbol{C}$ 的 k-嵌入,则 $\lambda L/\lambda K = \lambda L/K$ 是非分歧扩张(因 L/K 非分歧),故 $\lambda L \subset L$(Hilbert 类域定义),故 $\lambda L = L$. 其次易知 L/k 非分歧,故 K/k 是 L/k 的最大 Abel 子扩张. 记 $S = G(L/K)$则 G/S 是 G 的最大 Abel 商群,即知 $S = G'$ 是换位子群. 再注意,只需对 k 的素理想$\wp$证明$\wp O_K$ 是主理想,即$(\wp O_K, L/K) = 1$. 设$\wp O_K = \mathscr{P}_1 \cdots \mathscr{P}_g$, $\mathscr{P}_i$ 是 K 的素理想. $(\wp O_K, L/K) = \prod_i (\mathscr{P}_i, L/K)$,而$(\mathscr{P}_i, L/K) = (\sigma_i \mathscr{P}_1, L/K) = (\sigma_i \mathscr{P}_1, \sigma_i L/\sigma_i K) = \sigma_i (\mathscr{P}_1, L/K) \sigma_i^{-1}$. 故$(\wp, L/K) = \prod_{i=1}^{g} \sigma_i (\mathscr{P}, L/K) \sigma_i^{-1}$. 运用很复杂的纯群论方法可以证明这样的乘积总是等于 1,从而得到主理想定理(见[A—T]). □

以上证明引入"类域塔"问题: $K_0 \subset K_1 \subset K_2 \cdots$, K_i 是 K_{i-1} 的 Hilbert 类域. 直到 1964 年,由 Shafarevich 和 Golod 解决:当

$K_0=Q(\sqrt{-2\cdot3\cdot5\cdot7\cdot11\cdot13})$时类域塔可以无限长.

Q上的类域论值得特别讨论. $J=J_Q$ 可分解为

$$J\cong Q^*\times R^+\times\prod_p U_p,$$

即 idele $a=(a_\infty,a_2,a_3,\cdots,a_p,\cdots)=a_0(r,u_2,\cdots,u_p,\cdots)$，其中 $r\in R^+$(正实数)，$u_p\in U_p$($\mathbf{Q}_p$ 的单位群)，$a_0=(\text{sign }a_\infty)\prod_p p^{v_p(a)}\in Q^*$. 也可写为 $a=a_0ru_2u_3\cdots$.

由 § 9.8 系 2 新证明已知，对 $u_p\in U_p$ 有

$(u_p,Q(\zeta_{p^s})/Q)=u_p^{-1}:\qquad \zeta_{p^s}\longmapsto\zeta_{p^s}^{u_p^{-1}}$;

$(u_p,Q(\zeta_{q^t})/Q)=1$(当素数 $q\neq p$);

其中 $\zeta_{p^s}^{u_p^{-1}}=\zeta_{p^s}^{\alpha}$, $\alpha u_p\equiv1(\bmod p^s)$.

现设正整数 $m=\prod_p P^{s_p}$, $u=\prod_p u_p\in\prod_p U_p$, $\alpha_pu_p\equiv1(\bmod p^{s_p})$，则存在 $\alpha\in Q$ 使 $\alpha\equiv\alpha_p(\bmod p^{s_p})$对所有 $p|m$ 成立(孙子定理)，即 $\alpha\equiv u_p^{-1}(\bmod p^{s_p})$(所有 $p|m$)，故可记 $\alpha\equiv u^{-1}(\bmod m)$. 于是

$$\begin{aligned}(u,Q(\zeta_m)/Q)\zeta_m&=\prod_p(u_p,Q(\zeta_m)/Q)\prod_p\zeta_{p^{s_p}}\\&=\prod_p\zeta_{p^{s_p}}^{\alpha_p}=(\prod_p\zeta_{p^{s_p}})^{\alpha}=\zeta_m^{u^{-1}}.\end{aligned}$$

故若设 Q^{ab}为 Q 的最大 Abel 扩张，由添加诸单位根 ζ_m($0<m\in\mathbf{Z}$)到 Q 生成(Kronecker－Weber 定理)，则 Artin 映射给出同构映射 $\mathscr{A}$:

$$C_Q=J_Q/Q^*=R^+\times\prod_p U_p\stackrel{\mathscr{A}}{\longmapsto}G(Q^{ab}/Q)$$

$$r\cdot u\longmapsto u^{-1}:\qquad(\zeta\longrightarrow\zeta^{u^{-1}})$$

其中 ζ 为任一单位根(注意 $\mathscr{A}(r)=1$，因为 r 是任意次幂). 也

就是说 $\mathscr{A}$ 限制到 $\tilde{U}=\coprod_p U_p$ 上给出同构 $\tilde{U}\cong G(\boldsymbol{Q}^{ab}/\boldsymbol{Q})$, $u\to u^{-1}$.

定理 3 $\boldsymbol{Q}$ 的(有限)Abel 扩张 $K/\boldsymbol{Q}$ 与 $\tilde{U}=\coprod_p U_p$ 的(开)子群 H 间 1:1 对应,此对应由 Artin 映射 $\mathscr{A}$(限制到 $\tilde{U}$ 上)给出. 特别 $\tilde{U}\cong G(\boldsymbol{Q}^{ab}/\boldsymbol{Q})$. K 是 H(在 $G(\boldsymbol{Q}^{ab}/\boldsymbol{Q})$ 的象)的固定子域,$G(K/\boldsymbol{Q})\cong\tilde{U}/H$.

类域论理论体系完美,定理异常丰富深刻,为便于掌握运用及欣赏,现以诗(或称歌诀)概括之. 我们注意到,域 k 的 Abel 扩张集是一个格,象是枝干交错的一棵梅树;$\mathbf{J}_k$ 的子群格与之反向 1:1 对应,象是这树的冰面倒影.

近冰梅——类域论

疏影横钭近冰栽,枝枝簪雪映照来.
开为杏色偏芬洌,幽维菊风惯群莹.
稀世终久非歧寞,篱香于兹自主开.
纷纷谁解素宜主,类群甲群天安排.

分 句 释 义

1. k 的 Abel 扩域格{K}(疏影横钭近冰梅),由 Artin 映射而与其类群的闭子群格{H}(冰面照影)反向 1:1 对应.(基本定理)
2. 整体类域论包含局部类域论. Artin 映射限制到 v-分量(枝枝)则为局部映射(照),自成一系.(局部类域论)
3. k_v^*(开为杏)映为分裂(芬洌)群. $k_v^*\subset H\Leftrightarrow v$ 分裂.(分裂定

理）

4. U_v(幽维)映为惯性群.$U_v \subset H \Leftrightarrow v$ 不分歧.(分歧定理)

5. 希尔伯特(希氏)类域定义为最大非分歧(终久非歧寞)Abel扩张.(希氏类域)

6. 理想到希氏类域(篱香于兹)化为主理想.(主理想定理)

7. 完全分裂(纷纷解)于希氏类域的恰为 k 的素、主(素宜主)理想.(分解定理)

8. 类群与伽罗华群同构,理论妙美天成.(同构定理)

§9.12 类域构作与椭圆曲线复乘

类域的构作问题是 Hilbert 23 个问题中的第 12 个问题.经过近一个世纪的努力,只有很少进展.主要是用椭圆曲线的复乘法理论对虚二次域的类域的构作.不过此理论已对数论的发展起了很大的作用.下面简介.

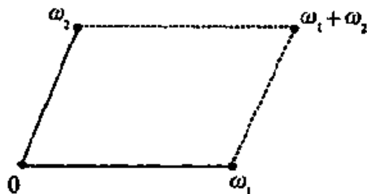
作为类域,分圆域的构作是很优美的(Kronecker-Weber 定理),即添加 ζ_n(n 次单位根即 x^n-1 的根)生成.能否像这样生成其它的类域呢？这就是 Kronecker 的"青春之梦".

复椭圆曲线 E 的方程可写为:

$$E: y^2=x^3+ax+b, \qquad (a,b,x,y \text{ 均在 } C \text{ 取值})$$

$\Delta=-16(4a^3+27b^2)\neq 0$ 称为其判别式,$j=-1728(4a)^3/\Delta$ 称为其 j-不变量.以 $E(C)$或 E 记 E 的复(坐标)点全体.可以适当定义 $E(C)$中的加法运算使之成为 Abel 群.群的单位元即是无穷远点 O,总认为 O 在 E 上.因 $x,y\in C$,若分开实虚部则有四个实变量,二个方程.故 E 的复点全体 $E(C)=E$ 拓扑上是一个曲面.容易证明 E 是一个环面.切开环面,$E(C)$同胚于一个平行四边形(对边视为相同).设其在复平面的顶点分别为 0, ω_1,

ω_2, $\omega_1+\omega_2$.



令 $L=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$ 为复平面 C 的格,则此四边形为 C/L (的代表元全系). 于是有同构

$$E \xrightarrow[\cong]{F} C/L$$

同构 F 可以明确写出为 $F: P \longmapsto \int_O^P \frac{dx}{\sqrt{x^3+ax+b}} \pmod L$. F 是 Riemann 面的复解析同构,也是(加法)Abel 群的同构.

另一方面,对于任意格 $L=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$,以 ω_1 和 ω_2 为周期的半纯复变量函数 f 称为椭圆函数,此时 f 可视为 C/L 上的函数. 最重要的椭圆函数是 Weierstrass $\wp$ -函数:

$$\wp(z,L)=\frac{1}{z^2}+\sum_{\substack{\omega\in L\\ \omega\neq 0}}\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2},$$

$\wp$在每个格点上有二阶极点. 可以证明,任一椭圆函数均可表为 $\wp(z)$和 $\wp'(z)$(微商)的有理函数.

引理 1 (1)对给定的 C 的任一格 L,有

$$\wp'(z)^2=4\,\wp(z)^3-g_2\,\wp(z)-g_3,$$

其中 $g_2=60\sum_{\substack{\omega\in L\\ \omega\neq 0}}\omega^{-4}$, $g_3=140\sum_{\substack{\omega\in L\\ \omega\neq 0}}\omega^{-6}$. 亦即 $(\wp(z),\wp'(z))$在一椭圆曲线上.

(2) $C/L \xrightarrow{\wp} E$: $y^2=4x^3-g_2x-g_3$

$z \longmapsto (\wp(z),\wp'(z))$, $\quad 0 \longmapsto O$

是 Riemann 面的复解析同构和 Abel 群的同构.

(3)每个复椭圆曲线 E 均可表为某 C/L 的同构象如(2). (详言之,给定 E:$y^2=4x^3-ax-b$,设 α,β 是 E 的拓扑一阶同调

群的生成元，$\omega_1=\int_\alpha \frac{dx}{y}$， $\omega_2=\int_\beta \frac{dx}{y}$， $L=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$，则

$$E \xrightarrow{F} \boldsymbol{C}/L, \quad P \longmapsto \int_O^P \frac{dx}{y} \mod L$$

即前述同构 F，也是上述(2)中 φ 的逆).

复椭圆曲线的自同态 由引理 1 可等同地视复椭圆曲线 E 为 $\boldsymbol{C}/L$. 设 L_1, L_2 为 $\mathbf{C}$ 的格，且有 $\alpha\in\boldsymbol{C}$ 使 $\alpha L_1\subset L_2$，则显然有椭圆曲线 $E_i=C/L_i$ 间的映射(数乘映射)

$$\varphi_\alpha: \quad C/L_1 \longrightarrow \boldsymbol{C}/L_2, \quad z \longmapsto \alpha z$$

引理 2 (i) $\boldsymbol{C}/L_1$ 到 $\boldsymbol{C}/L_2$ 的保 0 点不动的(全纯)解析映射只能是如上的数乘映射 φ_α.

(ii) $\{\varphi_\alpha | \alpha L_1\subset L_2\}$ 也就是复椭圆曲线 E_1 到 E_2 的所有保无穷点的有理映射.

(iii) $E_1\cong E_2 \Leftrightarrow \alpha L_1=L_2$，$\alpha\in\boldsymbol{C}^*$ (此时称 L_1 和 L_2 位似(homothetic)).

(iv) E 的自同态群 $\mathrm{End}(E)=\{\alpha\in\boldsymbol{C} | \alpha L\subset L\}$，

E 的自同构群 $\mathrm{Aut}(E)=\{\alpha\in\boldsymbol{C} | \alpha L=L\}$.

模变换 由上知复椭圆曲线同构类$\{E\}$(同构)与$\{\boldsymbol{C}/L\}$(位似)间 1∶1 对应. 设 $L=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$，位似于 $L_\tau=Z+\mathbf{Z}\tau$ ($\tau=\omega_1/\omega_2$)，$\tau\in\mathscr{H}$(复上半平面). 显然

$$L_\tau=L_{\tau'} \Leftrightarrow \tau'\in\Gamma(\tau)$$

这里 $\Gamma=SL_2(\mathbf{Z})=\{\gamma=\begin{pmatrix} a & b \\ c & d\end{pmatrix} | ad-bc=1\}$，$\gamma(\tau)=\frac{a\tau+b}{c\tau+d}$. 易证

$$\mathscr{H}/\Gamma=\{\tau\in\mathscr{H} \mid |\mathrm{Re}\tau|\leqslant\frac{1}{2},|\tau|\geqslant 1\}$$

故有下述各 1∶1 对应(E 的方程如引理 1)

$$\underset{\text{保}O\text{(双有理)同构类}}{\{E\}}\underset{(\wp(z),\wp'(z))}{\overset{F:P\mapsto\int_O^P\frac{dx}{y}}{\rightleftarrows}}\underset{L\text{位似类}}{\{C/L\}}\leftrightarrow\underset{\text{模}\Gamma\text{类}}{\{\tau\}}\leftrightarrow\{\tau\in\mathscr{H}/\Gamma\}\underset{\cong}{\overset{j}{\leftrightarrow}}C$$

$$j(E)=\frac{12^3a^3}{a^3-27b^2}=j(L)=\frac{12^3g_2^3}{g_2^3-27g_3^2}=j(\tau)$$

$$=\frac{1}{q}+744+\cdots(q=e^{2\pi i z})$$

可以证明 $E_1\cong E_2\Leftrightarrow j(E_1)=j(E_2)$

复乘法与类域 我们已经知道,若 $E=C/L$,则

$$\mathrm{End}(E)=\{\alpha\in C\mid\alpha L\subset L\}\supset \mathbf{Z}$$

如果 $\mathrm{End}(E)\neq\mathbf{Z}$(即$\exists\ \alpha\in C,\alpha\notin\mathbf{Z}$ 使 $\alpha L\subset L$),则称 E 有复乘.

现设 $\alpha L\subset L,\alpha\notin\mathbf{Z}$. $L=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2,\tau=\omega_1/\omega_2\in\mathscr{H}$ 则

$$\begin{cases}\alpha\omega_1=a\omega_1+b\omega_2\cdots\cdots(1)\\ \alpha\omega_2=c\omega_1+d\omega_2\cdots\cdots(2)\end{cases}\qquad(a,b,c,d\in\mathbf{Z})$$

即
$$\alpha\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}$$

故 α 是$\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}$的特征根(即满足 $\lambda^2-a_1\lambda+a_2=0$, $a_1=a+d,a_2=\det\begin{pmatrix}a\ b\\ c\ d\end{pmatrix}$). 即知 α 是二次代数整数,同时由(2)知

$$\alpha\in\mathbf{Q}(\tau)=K,$$

即 α 是虚二次域 $K=\mathbf{Q}(\tau)$的整数. 因 $\mathrm{End}(E)$是环,故 $\mathrm{End}(E)$是 O_K 的一个子环. 但 $\mathrm{End}(E)\supset\mathbf{Z}$,故其 $\mathbf{Z}-$秩为 2(否则若 $\mathrm{End}(E)=\mathbf{Z}\alpha$,则 $1=n\alpha,\alpha\in\mathbf{Q}$,矛盾). O_K 的 $\mathbf{Z}-$秩为 2 的子环称为**纲**(order). 当 E 变化时,$\mathrm{End}(E)$可取遍每个虚二次域的每个纲

R.（因 R 是一个格，令 $E_K=\boldsymbol{C}/R$，则显然 $\mathrm{End}(E_K)=R$）.

现设 K 是任一个虚二次数域. 我们要构作 K 的 Hilbert 类域. K 的任一分式理想 I 是 $\mathbf{C}$ 的一个格（I 是秩 2 的自由 Abel 群，设 $I=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$，则 $\tau=\omega_1/\omega_2\notin\boldsymbol{R}$，否则 $\tau\in K\cap\boldsymbol{R}=\boldsymbol{Q}$，则 ω_1 与 ω_2 在 $\mathbf{R}$ 上相关，在 $\boldsymbol{Q}$ 上也相关）. 复椭圆曲线 $\boldsymbol{C}/I$ 的自同态环显然即 O_K. 记 I 所在的理想类为

$$[I]=\{\alpha I\mid\alpha\in K^*\}.$$

故 $[I]$ 中每个理想（格）所对应的椭圆曲线 $\boldsymbol{C}/\alpha I$ 均与 $\boldsymbol{C}/I$ 同构. 即 K 的每个理想类 $\{\alpha I\}$ 定义一个椭圆曲线同构类 $\{\mathbf{C}/\alpha I\}$.

反之，设椭圆曲线 $E=\boldsymbol{C}/L$ 以 O_K 为自同态环，$L=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$，则 $\tau=\omega_1/\omega_2\in K$，故 $L_\tau=\boldsymbol{Z}+\boldsymbol{Z}\tau$ 是 K 的分式理想（(i)是 K 的加法子群；(ii)$O_KL_\tau\subset L_\tau$；(iii)分母有限）. 而 $E=\boldsymbol{C}/L\cong\boldsymbol{C}/L_\tau$.

定理 1 虚二次域 K 的分式理想类 $[I_1],[I_2],\cdots,[I_h]$ 与满足 $O_K=\mathrm{End}(E)$ 的椭圆曲线同构类 $\boldsymbol{C}/I_1,\cdots,\boldsymbol{C}/I_h$ 之间 1∶1 对应，从而对应 h（K 的理想类数）个不同的值 $j(I_1),\cdots,j(I_h)$（$j(I_i)=j(\boldsymbol{C}/I_i)$）称为域 K 的类不变量）.

定理 2 设 $I_1,\cdots,I_h$ 是虚二次域 K 的理想类的代表元系，则 $j(I_1),\cdots,j(I_h)$ 皆代数整数，且 $f(X)=(X-j(I_1))\cdots\cdots(X-j(I_h))$ 是K 上（也是 $\boldsymbol{Z}$ 上）不可约多项式.

定理 3 $K(j(I_1))=\cdots=K(j(I_h))$ 是 K 的 Hilbert 类域 K^H.

定理 4 $(I_1,K^H/K)j(I_2)=j(I_1^{-1}I_2)$.

这里 I_1,I_2 是 K 的二个不同理想类代表元（$(I_1,K^H/K)$ 是 Artin

符号).

定理 5 设 K 是虚二次域, j 是 K 的一个类不变量, E 为 $y^2=4x^3-\frac{27j}{j-12^3}(x+1)$, 即 $j(E)=j$, 则 K 的最大 Abel 扩张为

$$K^{ab}=K(j,x),$$

x 过 E 的有限阶点的横坐标(这里设 $j\neq 0$, 1728).

注意上述 x 实则为双周期函数 $\wp(z)$ 的取值. 这与 Kronecker—weber 定理很类似: $\boldsymbol{Q}$ 的最大 Abel 扩张 (即分圆域的复合)为 $\boldsymbol{Q}^{ab}=\boldsymbol{Q}(\zeta)$, ζ 过单周期函数 $e^{2\pi iz}$ 的取值.

若 E 是有理系数椭圆曲线 E: $y^2=4x^3-ax-b$, $a,b\in\boldsymbol{Q}$. 设 K 的整数环 $O_K=\mathrm{End}(E)$. 因 $j(E)=\frac{12^3a^3}{a^3-27b^2}\in\boldsymbol{Q}$, 故 K 的 Hilbert 类域 $K^H=K(j(E))=K$, 故 $h(K)=1$. 由定理 1 知此时每个 K 决定唯一的(同构意义下) $E=\boldsymbol{C}/I$, (I 为 K 的任一理想). 反之, 若 K 为类数 $h(K)=1$ 的虚二次域. 则 K 决定的唯一(同构意义下) $E=\boldsymbol{C}/I$, 也是以有理系数方程定义的(由定理 2 知 $j\in\mathbf{Z}$, 故 E 同构于 $y^2=4x^3-\frac{27j}{j-12^3}(x+1)$). 总之有

系 1 同态环 $\mathrm{End}(E)$ 为某虚二次域 K 的整数环 O_K 的**有理系数**椭圆曲线 E 在复同构意义下只有 9 个, 恰对应于 $h(K)=1$ 的 9 个虚二次域 $K=(\sqrt{-d})$,

$$d=1,2,3,7;11,19,43,67,163.$$

类似还可得到:

系 2 具有复乘的**有理系数**椭圆曲线 E 在复同构意义下只有 13 个, 除上述系 1 中 9 个外, 还有(记 $\mathrm{End}(E)\subset O_K$, $K=\boldsymbol{Q}$

$(\sqrt{-d})$：

$$\mathrm{End}(E)=\mathbf{Z}+2O_K: \qquad d=1,3,7$$
$$\mathrm{End}(E)=\mathbf{Z}+3O_K: \qquad d=3.$$

与类域密切相关的是 Genus 域（种域）. 数域 k 的 Genus 域 $\tilde{K}$定义为 k 的最大非分歧（在有限素除子）扩张且 $\tilde{K}=kk_1$，$k_1/\boldsymbol{Q}$ 是 Abel 扩域（Fröhlich）. 在〔Zh13〕中用类域论证明了，任一数域 k 的 Genus 域为

$$\tilde{K}=k\prod_p \Omega^{(p)}$$

其中 $\Omega^{(p)}$按 $\boldsymbol{Q}$ 上的类域论对应于 $\bar{U}=\prod_{p\neq\infty}U_p$ 的子群 $H_p\prod_{q\neq p}U_q$，$H_p\subset U_p$ 由$\{N_{k_\wp/Q_p}(U_\wp)\}$生成（p 过分歧素数，$\wp$过 p 在 k 素因子）. 特别 $G(\Omega^{(p)}/\boldsymbol{Q})\cong U_p/H_p$. 当 $p\neq2$ 时 $\Omega^{(p)}$是 $\boldsymbol{Q}$ 的 $\mathrm{GCD}_\wp(U_p:NU_\wp)$次循环扩张.

当 k 为 Abel 数域时，其 Genus 域 $\tilde{K}$即为含 k 的最大绝对 Abel 域且在 k 的所有有限素除子上非分歧.〔Zh6〕用较简单方法构作了 $\tilde{K}$：当 k 次数为素数幂 q^t 时，其 Genus 域为

$$\tilde{K}=k\prod_{p\neq q}C_p=\prod_p C_p$$

其中 p 过在 k 分歧的素数，C_p 是 $\boldsymbol{Q}(\zeta_p)$的唯一 $e(p)$次子域（$p\neq q$ 时），C_q 是 $\mathbf{Q}(\zeta_{q^t})$的 $e(q)$次子域（某 t），$e(p)$是 p 在 k 的分歧指数. 此文还具体构作了（2，⋯，2）型域等的 Genas 域.

二次域的 Genns 理论很古典. 可用以决定类群的 2－秩（对代数函数域的情形见〔Zh14〕）. 还可用以决定四次扩张的结构、相对整基的存在等（〔Zh7〕）.

利用 Kronecker—Weber 定理研究 Abel 域是最常用的方法. 对四次域见〔F1〕,五次域见〔zhao〕,相关的见〔P—F〕,〔F2〕(类数奇偶性). 局部类域论与形式群很有关系(见〔Li〕). 〕

最后对 Fermat 大定理的证明稍作介绍. A. Wiles 的证明原文见〔Wi〕. 简介可见〔Zh21〕. 首先,$\boldsymbol{Q}$ 上的椭圆曲线 E 就是由如下方程定义的非奇异曲线:

$$E:\quad y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \qquad (a_i\in\mathbf{Z})$$

无穷远点 $O=(\infty,\infty)$ 总视为 E 上点. 对于素数 p,以 $E(\boldsymbol{F}_p)$ 记 $\boldsymbol{E}$ 在 $\boldsymbol{F}_p$ 上点全体(即上述方程 $\bmod p$ 解全体),并记 $a_p=p+1-\#\boldsymbol{E}(\boldsymbol{F}_p)$.

对正整数 N,考虑 $\Gamma=SL_2(\mathbf{Z})$ 的子群

$$\Gamma_0(N)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}: c\equiv 0(\mathrm{mod}N), ad-bc=1\right\}.$$

复上半平面 $\mathscr{H}$ 上的全纯函数 $f(z)$ 称为权为 k 的对于 $\Gamma_0(N)$ 的模形式是指

$$f(\gamma(z)))=(cz+d)^k f(z)$$

对所有 $\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma_0(N)$, $z\in\mathscr{H}$ 成立,且在∞全纯. 若还满足 $f(\infty)=0$ 则 f 称为尖点形式.

椭圆曲线 E 称为是模的(或模椭圆曲线),是指存在着对于某 $\Gamma_0(N)$ 的权为 2 的尖点模形式

$f(z)=\sum_{n=0}^{\infty}c_n\exp(2\pi inz)$ 使得

$$c_p=a_p=p+1-\#E(\boldsymbol{F}_p)$$

对于除有限个之外的所有素数 p 成立. ($f(z)$ 还会是 Hecke 变换的特征形式). 这也相当于从 $\mathscr{H}/\Gamma_0(N)$ 的紧致化到 E 有一

个全纯映射.

谷山丰(Taniyama),志村五郎(Shimura)在1955年提出猜想:$\boldsymbol{Q}$ 上所有椭圆曲线都是模的. 1971年Shimura证明此猜想对有复乘的 $\boldsymbol{Q}$ 上椭圆曲线成立. 1985年,G. Frey断言:谷山丰猜想蕴含Fermat大定理. 即断言:若 $a^n+b^n=c^n$ 对非零 $a,b,c\in\boldsymbol{Z}$ 成立,则椭圆曲线

$$y^2=x(x+a^n)(x-b^n) \qquad (*)$$

不是模的. 1986年K. Ribet证明了Frey的断言. *A. Wiles* 闻此而潜心研究8年,终于在1994年9月19日证明了谷山丰猜想的一部分,即证明了包括(*)式(如果存在的话)的一类椭圆曲线是模的,从而证明了 *Fermat* 大定理. *Wiles* 的出发点是E[3],即E的3-分点. 易知 $E(3)=\boldsymbol{F}_3\oplus\boldsymbol{F}_3$ 是两个3阶循环群的直和(因为 $E(\boldsymbol{C})$ 等同于平行四边形如前述),即 $E(3)$ 是 $\boldsymbol{F}_3$ 上2维线性空间. 故 $E[3]$ 的(由Galois同构引起的)线性变换可表示为 $\boldsymbol{F}_3$ 上2阶方阵($\boldsymbol{F}_3$-表示 ρ_0). 而Tunnell－Langlands曾证明 $E[3]$ 是模的(即 $c_p\equiv a_p \pmod 3$ 对所有素数 $p\neq 3$ 成立). 然后Wiles考虑 3^n-分点全体 $E[3^n]$,取反向极限而得3-adic表示 ρ_E,从而由 $E[3]$ 是模的出发,曲折地导出 E 是模的,完成了对Fermat大定理的历史性证明.

参 考 文 献

[A1] E. Artin. 1950～1951. Algebraic Numbers and Algebraic Functions, Lecture Notes, Princeton University and New York University.

[A-T] E. Artin and J. Tate. 1967, Class Field Theory, Benjamin, New York.

[At] M. Atiyah, I. Macdonald. Introduction to Commutative Algebra. Addison-Wesley, London, 1970.

[Ba] A. Baker. 1969. On the class number of quadratic fields, Bull. Lon. Math. Soc., 1: 98～102.

[F1] 冯克勤. 1984. 四次循环域的明显刻画. 数学学报, 27: 410～424.

[F2] 冯克勤, 1982. An elementary criterion on parity of class number of cyclic number fields. Scientia Sinica, 25: 1032～1041.

[F3] 冯克勤. 代数数论入门. 上海科学技术出版社, 1988.

[F4] 冯克勤. 交换代数基础. 高等教育出版社, 1985.

[Ha] R. Hartshorne. Algebraic Geometry. Springer-Verlag, Berlin, 1977.

[He] E. Hecke. Lectures on the Theory of Algebraic Numbers. Springer-Verlag, Berlin. 1981.

[Hua] 华罗庚. 数论导引. 科学出版社. 1979.

[Iy] S. Iyanaga, The Theory of Numbers. North-Holland, Amsterdam. 1975.

[Ke] 柯召, 孙琦. 数论讲义. 高等教育出版社, 1986.

[La] S. Lang. 1986. Algebraic Number Theory, (GTM 110)

Springer-Verlag, Berlin.

[Li] 李德琅. 1989. Formal groups and local field theory. Chin. Ann. Math. 10B, 2: 241～260.

[Liw] W. C. Winnie Li. Number Theory with Applications, World Sci. Singapore, 1996.

[Lo] R. Long. Algebraic Number Theory. Marcel Dekker, New York, 1977.

[Lu] 陆洪文. 1982. Congruences for the class number of quadratic fields. Abh. Math. Sem. Univ. Hamburg, 52: 254～258.

[Lu2] 陆洪文. 二次数域的高斯猜想. 上海科学技术出版社, 1995.

[Ma] D. Marcus. Number Fields. Springer-Verlag, Berlin, 1977.

[Ne] J. Neukirch. Class Field Theory. Springer-Verlag, Berlin, 1986.

[Pan] 潘承洞, 潘承彪. 初等数论. 北京大学出版社, 1992.

[P-F] 裴定一, 冯克勤. 1980. 分圆单位的独立性. 数学学报, 20: 7773～7778.

[Sa] P. Samuel. Algebraic Theory of Numbers. Hermann. Houghton Mifflin, Boston, 1970.

[Si] J. H. Silverman, The Arithmetic of Elliptic Curves. Springer-Verlag, 1986.

[Si2] J. H. Silverman. Advanced Topics in the Arithmetic of Elliptic Curves. Springer-Verlag, 1994.

[St] H. M. Stark. 1967. A Complete determination of the complex qnadratic fields of class namber 1, J. Michigam

math, 14: 1～27.

[Wang] 王元. 华罗庚. 开明出版社, 1994.

[Wa] L. C. Washington. Introduction to Cyclotomic Fields, 2nd ed. Springer-Verlag, Berlin, 1997.

[We] E. Weiss. Algebraic Number Theory, McGraw-Hill. New York, 1963.

[Wi] A. J. Wiles. 1995. Modular elliptic curves and Fermat's Last Theoren. Annals of Math., 141: 443～551.

[Wei] A. Weil. Basic Number Theory. Springer-Verlag, New York, 1968.

[Zhl] 张贤科. 1982. (2,2,…,2)型数域. 中国科学技术大学学报, 12, No. 4: 29～41.

[Zh2] 张贤科. 1992. 实二次域类数 $h(K)=1$ 问题. 科学通报, 37, No. 22: 2017-2019.

[Zh3] 张贤科. 1988. Class numbers and units of several kinds of quadratic fields. Presented at the Centennial of American Math. Soc., Providence.

[Zh4] 张贤科, 劳. 华盛顿. 1997. 实二次域的理想类群与其子群. 中国科学, A27, 6: 522～528.

[Zh5] 张贤科. 1989. Congruences mudulo 2^3 for class numbers of general quadratic fields Q ($\sqrt{m}$) and Q ($\sqrt{-m}$), J. of number theory, 32, No. 3: 332～338.

[Zh6] 张贤科. 1985. A simple construction of genus fields of abelian number fields. Proceed. American Math. Soc. 94, No. 3: 393～395.

[Zh7] 张贤科. 1984. Cyclic quartic fields and genus theory of

their subfields. J. of Number Theory. 18, No. 3:350～355; Math. Rev. 85k:11053.

[Zh8] 张贤科. 1996. 阿贝尔 q-域的分类和素理想分解. 科学通报, 41, No. 22:2113～2115.

[Zh9] 张贤科. 1996. 阿贝尔 q-域的相对整基. 科学通报, 41, No. 12:1066～1068.

[Zh10] 张贤科. 1995. 实二次域的方程与半单和最小连分数. 科学通报, 40, 10:865～867.

[Zh11] 张贤科. 1987. 一般三次循环数域的类数同余公式. 中国科大学报, 17, 2:141～145.

[Zh12] 张贤科, 1988. 一般四次循环域的十个 Ankeny-Artin-Chowla 型类数公式. 中国科学, A7, No. 7:688～697.

[Zh13] 张贤科. 1986. Counterexample and correction about genus fields of number fields. J. of number theory, 23, No. 3:318～321.

[Zh14] 张贤科. 1987. Ambigous classes and 2-rank of class groups of quadratic function fields. J. China Univ. Sci. Tech. 17, No: 4, 425～430.

[Zh15] 张贤科. 1992. Determination of solutions and solvabilities of Diophantine equations and quadratic fields. Algebraic Geometry and Algebraic Number Theory, S. S. Chern & Feng Keqin(ed.), World Science, Singapore/London, 3:189～199.

[Zh16] 张贤科. 1983. (2, 2, …, 2)型数域的密度. 中国科学, A9:805～811.

[Zh17] 张贤科. 1984. $(l, l, \cdots, l)$型数域. 中国科学, Al:31～38.

[Zh18] 张贤科. 1986. $(l,l,\cdots,l)$型数域的相对整基和单位. 数学学报, 29, No. 5: 622～627.

[Zh19] 张贤科. 1988. (2,2,…,2)型代数函数域. 中国科学, A1: 8～16.

[Zh20] 张贤科. 1988. 决定类数为一的(2,2,…,2)型代数函数域. 中国科学, A2: 129～135.

[Zh21] 张贤科. 1997. 费尔马大定理——怀尔斯的证明. 世界科技研究与发展, Vol. 19, No. 1: 74～78.

[Zh22] 张贤科. 高等代数学. 清华大学出版社, 1998.

[Zhao] 赵春来. 1984. 五次绝对循环数域中的基本单位. 中国科学, A27: 27～40.

名 词 索 引